ALL CAMPUSES

STUDENT CATALOG
2024-2026

MYCOMPUTER CAREER
TRAINING FOR A BETTER LIFE

Branches and Affiliated Campuses

MyComputerCareer at Raleigh Main Campus
(919) 301-0951
5511 Capital Center Dr. Suite 500
Raleigh, NC 27606

MyComputerCareer at Charlotte branch
(704) 302-1031
3701 Arco Corporate Dr. Suite 115
Charlotte, NC 28273

MyComputerCareer at Arlington branch
(817) 210-6308
1701 E. Lamar Blvd. Suite 250
Arlington, TX 76006

MyComputerCareer at Dallas branch
(214) 646-3973
12225 Greenville Ave. Suite 500
Dallas, TX 75243

MyComputerCareer at North Houston branch
(281) 245-0888
7908 N Sam Houston Pkwy W Ste. 300
Houston, TX 77064

MyComputerCareer at Sugar Land branch
(832) 939-3980
14141 SW Freeway Ste. 1010
Sugar Land, TX 77478

MyComputerCareer at Columbus Main Campus
(614) 891-3200
4349 Easton Way Suite 145
Columbus, OH 43219

MyComputerCareer at Las Vegas branch (Nellis Air Force Base)
(702) 659-7652
4475 England Ave. Bldg. #20
Nellis AFB, NV 89191

MyComputerCareer at Columbus Non-Instructional Branch
(919) 278-7944
Apex, North Carolina

MyComputerCareer at Indianapolis Main Campus
(317) 550-3044
2601 Fortune Cir East Ste.100c
Indianapolis, IN 46241

Website – www.mycomputercareer.edu

Mailing Address for all campuses:
1321 Upland Dr. PMB 8542
Houston, Texas 77043

Table of Contents

Governing Board of Directors

James A. Galati – Chairman of the Board, Amy Onuska – CEO, Bruce Ackerman – Chief Marketing Officer, Dan Pryor – Chief Placement Officer, Matthew Mosley – Secretary. James A. Galati (96.39%) and Amy Onuska (3.61%) are the owners of the institution.

Class B nonvoting ownership percentages are as follows: James Galati 46.05% (51.08% total), James A. Galati Legacy Trust 26.77% (24.10% total), Ravenclaw Haven Trust 23.57% (21.21% total) and Amy Onuska 3.61% (3.61% total).

Mission Statement

Our mission at MyComputerCareer is to help our students develop the skills necessary to permanently and positively change their lives and futures by attaining financially rewarding and personally fulfilling careers in Information Technology.

Accreditation and State Governing Authority

MyComputerCareer is accredited by ACCET, the Accrediting Council for Continuing Education and Training. ACCET is listed by the U. S. Department of Education as a nationally recognized accrediting agency. You may request electronic or paper copies of our Accreditation and/or State license activity by emailing Compliance@mycomputercareer.edu.

Campuses located in the State of North Carolina are licensed by the North Carolina State Board of Community Colleges.
The North Carolina State Board of Community Colleges is not an accrediting agency.
North Carolina Community College System ~ 200 W Jones St. Raleigh, NC 27603

The governing authority of MyComputerCareer locations in the State of Texas is:
Texas Workforce Commission Career Schools and Colleges ~ 101 East 15th Street Room 104T Austin, Texas 78778-0001

The governing authority of MyComputerCareer in the state of Ohio is:
Ohio State Board of Career Colleges and Schools ~ 30 East Broad Street, Suite 2481Columbus, OH 43215
School Registration Number 12-03-1987T

This institution in the State of Indiana is authorized by:
Indiana Commission for Higher Education - Indiana Board for Proprietary Education
101 West Ohio Street, Suite 300 Indianapolis, Indiana 46204-4206 • 317.464.4400

Campus Hours

Students are required to attend two classes per week at the institution. Evening schedules have an additional Learning Lab each week. Students will be scheduled at enrollment to attend a specific class schedule. Breaks will be held as deemed necessary by the instructor with no more than one ten-minute break per class hour. An instructor is available outside of class throughout the day. See hours below and/or posted on the campus

Lecture & Lab Schedule Monday – Thursday

Morning	9:30am – 3:30pm
Evening	6:00pm – 11:00pm + 2 hr. Learning Lab

IDL Lecture & Lab Schedule Monday – Thursday EST

Monday	10:00am – 4:00pm
Evening	6:00pm – 11:00pm or 6:30pm – 11:30pm 7:00pm – 12:00am + 2hr. Learning Lab

Addtl. CSS & CSE Schedule – 6:30pm – 11:30pm EST

Associate Degree Schedule – 6:30pm – 8:45pm EST
tutoring available 8:45pm – 9:40pm EST Tues. & Thurs.

Campus Lab Hours (check campus posting for any updates)

Raleigh	M-Th 2pm – 11pm; Sat 9am – 3pm	Houston	M-Th 2pm – 11pm; Sat 9am – 3pm
Charlotte	M-Th 2pm – 11pm; Sat 9am – 3pm	Columbus	M-Th 3pm – 11pm;
Arlington	M-Th 2pm – 11pm	Indianapolis	M-Th 2pm – 11pm;
Dallas	M-Th 2pm – 11pm; Sat 9am – 3pm	Remote Sched	M-Th 10am–10pm; F-Sat 9am – 3pm

Facilities

MyComputerCareer at Raleigh LLC, MyComputerCareer at Charlotte LLC, MyComputerCareer at Arlington LLC, MyComputerCareer at Dallas LLC, MyComputerCareer at North Houston LLC, MyComputerCareer at Sugar Land LLC, MyComputerCareer at Columbus LLC and MyComputerCareer at Indianapolis LLC are wholly owned subsidiaries of MyComputerCareer Inc. James A. Galati (96.39%) and Amy Onuska (3.61%) are the Class A owners of the institution. All facilities are compliant with the 2010 ADA Standards for Accessible Design. Should a student need specific physical or intellectual accommodations, prospective student should refer to the Policy on Non-Discrimination. Facilities have cameras in the classrooms to record for quality assurance and internal training purposes only. Online classes are also recorded for the same purposes. The recordings are not available for public distribution or student access.

Raleigh: MyComputerCareer is located in the Capital Center at 5511 Capital Center Drive, Suite 500, Raleigh, NC 27606. The student facilities consist of one large classroom, a kitchen area with a refrigerator, and a large break/study area. Classrooms are designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 is followed. Policy guidelines for use of school property will be posted in a common area within the school.

Arlington: MyComputerCareer is located at 1701 Lamar Blvd., Suite 250, Arlington, TX 76006. The student facilities consist of one large classroom, a kitchen area with fridge, and a large break/study area. The classroom is designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 per class is followed. Students may visit with their instructors during predetermined office hours. Policy guidelines for use of school property will be posted in a common area within the school.

Charlotte: MyComputerCareer is located in the 3701 Arco Corporate Drive, Suite 115, Charlotte, NC 28273. The student facilities consist of one large classroom, a kitchen area and a break/study area. Classroom is designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 is followed. Policy guidelines for use of school property will be posted in a common area within the school.

Dallas: MyComputerCareer is located at 12225 Greenville Ave, Suite 500, Dallas, TX 75243. The student facilities consist of two large classrooms, a kitchen area with a refrigerator, and a large break/study area. Students may also have access to a café located in the building, depending on hours set by the café management. The instructors primarily work area is in the classroom. Students may visit with their instructors during predetermined office hours. Classrooms are designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 per class is followed. Policy guidelines for use of school property will be posted in a common area within the school.

North Houston: MyComputerCareer is located at 7908 North Sam Houston Parkway West, Suite 300, Houston, TX 77064. The student facilities consist of three large classrooms, a kitchen area with a refrigerator, and a large break/study area. The instructors primarily work in the classroom and also have an office located near the classroom. Students may visit with their instructors during predetermined office hours. Classrooms are designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 per class is followed. Policy guidelines for use of school property will be posted in a common area within the school.

Sugar Land: MyComputerCareer is located at 14141 SW Freeway Ste. 1010 Sugar Land, TX 77478. The student facilities consist of four classrooms, a flextime area, and a break room for students. Classrooms are designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 per class is followed. Instructors are available to provide personal instruction as students develop their hands-on skills. A licensed testing facility is also on-site. Policy guidelines for use of school property will be posted in a common area in the school.

Columbus: The MyComputerCareer is located at 4349 Easton Way Suite 145 Columbus, OH 43219. The 4,125 sq. ft. facility consist of one classroom, a flextime area, and a break area for students. The classroom is designed to accommodate students with a student to equipment ratio of 1:1 with a maximum capacity of 30 students. A student to instructor maximum ratio of 30:1 per class is followed. Instructors are available to provide personal instruction as students develop their hands-on skills. Policy guidelines for use of school property will be posted in a common area within the school.

Indianapolis: The MyComputerCareer is located at 2601 Fortune Circle East Suite 100c Indianapolis, IN 46241. The student facilities consist of two classrooms and a break room for students. Classrooms are designed to accommodate students with a student to equipment ratio of 1:1. A student to instructor maximum ratio of 30:1 per class is followed. Instructors are available to provide personal instruction as students develop their hands-on skills. A licensed testing facility is also on-site. Policy guidelines for use of school property will be posted in a common area within the school.

Enrollment Policies and Guidelines

Students must meet with a member of the Admissions Team to be considered for acceptance into our programs. The Admissions Team member will ascertain the prospective students' ability to enroll in a program during the admissions process. MyComputerCareer will determine acceptance into any offered program. The decision to allow a student to enroll in the program will also be guided by the standards for each State below. Additionally, a student will need a government issued ID to verify identity and pass an internet speed test to ensure network and personal computers are adequate. 2MB upload and download is the minimum. The CSS and CSE program have prerequisite requirements that are outlined in the "Enrollment Prerequisites" section on page 26. Any prospective student who has a special needs request or accommodation must submit the request in writing via email to their Admissions Advisor prior to enrollment to determine if the school can accommodate the request.

State of North Carolina

- Documentation of one of the following is required for enrollment: High School transcript, copy of the certificate of high school equivalency, transcript showing graduation from a community college or university that operates in compliance with state or local law, completion of secondary education equivalent to high school education in the United States or in extenuating circumstances a signed, notarized attestation of graduation from any of the above. VA benefit enrollment requirements may vary. Please consult with your Admissions team for those requirements. Not applicable for Avocational courses.
- There is a minimum age requirement of 17 for enrollment into any program at MyComputerCareer. Applicants under the age of 18 need a parent or guardian's signature in addition to their own signature on the Enrollment agreement.

State of Texas

- High School Completion, GED or equivalent or College Degree is required for enrollment. Proof of attainment must be supplied, and a copy will be kept in the student's file. Not applicable for Avocational Seminar courses.
- There is a minimum age requirement of 17 for enrollment into any program at MyComputerCareer. Applicants under the age of 18 need a parent or guardian's signature in addition to their own signature on the enrollment agreement.

State of Ohio

- High School Completion, GED or equivalent or College Degree is required for enrollment. Proof of attainment must be supplied, and a copy will be kept in the student's file. Not applicable for Avocational courses.
- There is a minimum age requirement of 17 for enrollment into any program at MyComputerCareer. Applicants under the age of 18 need a parent or guardian's signature in addition to their own signature on the enrollment agreement.
- All students who are accepted for enrollment will be given a copy of the student catalog at the time of enrollment that lists the graduation and placement rates for the program they are entering for each of the preceding three yrs.

State of Indiana

- High School Completion, GED or equivalent or College Degree is required for enrollment. Proof of attainment must be supplied, and a copy will be kept in the student's file. Not applicable for Avocational courses.
- There is a minimum age requirement of 17 for enrollment into any program at MyComputerCareer. Applicants under the age of 18 need a parent or guardian's signature in addition to their own signature on the enrollment agreement.

VA Benefits Enrollment Policy – All Campuses

MyComputerCareer follows the requirements as listed in PL 115-407 Section 103 and 104 Compliance: Title 38 USC 3679 (e). As an institution, MyComputerCareer does not impose any penalty, including assessment of late fees, the denial of access to classes, libraries, or other institutional facilities, or the requirement that a covered individual borrow additional funds while awaiting payment of VA funds under chapter 31 and 33. A student requesting to use benefits must submit a COE before the first day of class, sign the Memorandum of Understanding to use such entitlement, provide additional information necessary to certify enrollment, and may impose a fee for the amount that is different between the VA payment.

Policy on Non-Discrimination

MyComputerCareer does not discriminate nor condone discrimination on the basis of sex, religion, nationality, ethnic origin, color, race, age, disability, sexual orientation, or any other legally protected characteristic. Our facilities are handicap accessible. Students with special needs may need to meet minimum mobility requirements for testing of the companies issuing the certification. Students with special educational needs should notify their Admissions Representative before enrolling so the institution can make an effort to accommodate the needs

Transfer of Credit Policy

MyComputerCareer will consider credit for previous training and education that a student has received at another institution that is related to the program in which they are enrolled. The student must notify their Admissions Representative, prior to enrollment, of previous training or education that they would like to have considered for transfer. Any courses to be considered must have been passed with a "C" (70%) or better and must be from an accredited institution or provided by the U.S Military. Transcripts must be provided at the time of the request. Students seeking credit for any course that provides training towards a certification must provide proof that they have passed the Industry certification exam that is still active and must pass an equivalent course practice exam with a 90% or better. General Education courses in the Associates Degree program do not require an exam for transfer credit review. A member of the Transfer Credit Review Committee will review the documentation provided to arrive at a final decision. If credit is awarded, the tuition will be reduced by a prorated amount, and the program length will be adjusted. If transfer credit is denied, an appeal must be submitted to the Site Coordinator within five business days of the denial and prior to the start of classes. No fees will be assessed for the evaluation of transfer credit. Transfer credits from other institutions may not exceed 50% of the program. Courses accepted for Transfer of Credit may affect financial aid such as prorating the overall aid package based off the Quarter Credit Hours remaining after the Transfer of Credit is applied. Please see a Financial Aid representative for questions or more information.

All Credits earned at MyComputerCareer are eligible for transfer credit at any MyComputerCareer location, therefore the proof of certification and practice exam requirement outlined above is not needed for alumni.

MyComputerCareer will assist students wishing to transfer credits to another school by, for example, providing transcripts, syllabi, student catalog, etc. Requests can be made at any time by emailing the Site Coordinator. Clock or Credit hours earned at the institution will in all likelihood not transfer to another institution. Students should check with their transferring institution to determine if credits are likely to transfer. Military students seeking to use their veteran's benefits must provide their written transcript of previous training and education for evaluation for credit prior to enrollment at the school. Any schools with articulation agreements with MyComputerCareer will be listed with the program and campus where the articulation agreement exists.

Tuition Payment

MyComputerCareer accepts tuition payment in the form of check, money order, credit card and student loans where available. Payments at the Raleigh, NC and Charlotte, NC campuses can only be received up to 50% of the total tuition prior to the program's midpoint. The remainder of the tuition may be collected only when the student has completed one-half of the program. The Columbus, OH campus defers the collection and application of federal, state or local government funds in the manner as controlled by the applicable federal, state or local regulations. Student loans or other financial aid funds received from private entities including, but not limited to, banks, financing companies, credit card companies, and other lending sources must be collected or disbursed in the following manner: 1. Loans or other financing payments for amounts less than five thousand dollars may be disbursed as a single disbursement, regardless of course length. 2. Loans or other financing payments for amounts greater than five thousand dollars that reflect a class term less than six months must have two equal disbursements. The disbursement schedule is as follows: one-half of the tuition amount released initially, and the remainder released half way through the course term. 3. Loans or other financing payments for amounts greater than five thousand dollars that reflect a class term greater than six months, but less than twelve months must have three equal disbursements. The disbursement schedule is as follows: one-third of the tuition amount released initially, the second disbursement will be released one-third of the way through the length of the training, and the remainder released two-thirds of the way through the course term. MyComputerCareer accepts the following Federal Student Aid:

- Federal Pell Grants
    - A Pell Grant is awarded based on need and don't have to be repaid. They can be awarded to students who have not yet earned a bachelor's degree. The maximum Pell Grant award for the 2020/21 award year is $6345, however, the actual award depends on the student's financial need (Estimated Family Contribution / EFC), the Cost of Attendance and the length of the academic year in which the student is enrolled. Not all students qualify.
- William D. Ford Federal Direct Loans - Loans that must be repaid plus interest
    - Subsidized Loans - Based on financial need. The federal government pays interest while the student is in school and during deferment.
    - Unsubsidized Loans - Based on the student's education costs and other aid received. Interest accrues immediately.
    - Direct Plus Loans – Available to parents of dependent students. They are unsubsidized.

Eligible Title IV disbursements will be made at the beginning of each program except for Direct Loans, which are delayed by 30 days from the first day of the payment period, and again at the program midpoint once the student has successfully completed the credit hours attempted in the payment period and half of the academic year in instructional weeks (i.e., 15 weeks or 21 weeks). Title IV disbursements for the Associate Degree program on the Columbus, OH campus occur at the end of each payment period when the student has successfully completed the weeks of instruction in the payment period and 18 quarter credits.

MyComputerCareer also accepts WOIA & TAA vouchers, GI Bill® and other Military funding sources, and other state and federal grants and scholarship programs. (GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government Web site at http://www.benefits.va.gov/gibill.) Tuition payment must be arranged or received before the 1st day of the scheduled start of their program. Financial institutions providing student loans may be given other payment terms and may charge their own fees for lending including interest, origination fees, and any and all other fees any institution may charge. Student loan applications are available through the Admissions Director or Financial Counselor if you don't seek private lending on your own. For more information about private lending options please visit the Financial Aid Disclosures and Application Process section at https://www.mycomputercareer.edu/additional-disclosure-statements/.

MyComputerCareer has no control over the fees charged by lending institutions. Any funds that are not paid at the time of obligation by the student are subject to collection. Additionally, students are subject to termination for nonpayment. MyComputerCareer will attempt to recover the funds from the student prior to turning the debt over to a collection agency. Institutional scholarships and/or grants where applicable are outlined in the campus specific section at the end of this catalog. MyComputerCareer will also charge a $50.00 service fee for any returned checks that are given to the school as payment for tuition.

Scarlett Scholarship: An annual scholarship to a Veteran, Veteran Spouse or Veteran Dependent with no military benefits remaining or has never had benefits to use for education. Must meet the general admission requirements outlined above, complete the application with an essay and provide verification of military affiliation. The Scholarship recipients will be chosen each year by Scarlett's parent. To learn more visit https://www.mycomputercareer.edu/scarlettsscholarship/.

Alumni General Education Grant – (Enrollments after 1/1/2025) MyComputerCareer alumni who graduated from two certificate programs at any of our locations will be awarded a grant to cover the tuition for the general education courses in the Associate of Applied Science in IT Network Administration and Security program.

Certification Mastery Course Grant – A full Tuition grant for students enrolled in a MyComputerCareer Program at any location. Student must enroll and start within the maximum time frame of their Active program. Mastery Courses are avocational and outlined in the Student Program section of this catalog.

Title IV Credit Balance

Whenever MyComputerCareer disburses Title IV funds by crediting a student's account and the total amount of **ONLY** Title IV funds credited exceeds the amount of tuition, fees and other authorized charges assessed to the student, the excess is considered a Title IV Credit Balance. Title IV Credit Balances will be paid to the student or parent within 14 days of the disbursement that created the excess or as per instructions supplied by a completed "Authorization to Hold or Release Funds" form.

Title IV Overage

Whenever MyComputerCareer disburses Title IV funds *and/or other sources of funding* by crediting a student's account and the total amount of ALL funds credited exceeds the amount of tuition, fees and other authorized charges assessed to the student, the excess that is not a Title IV Credit Balance is considered an Overage. Overages will be evaluated and paid to the student or parent according to the timeline specified below or as per instructions supplied by a completed "Authorization to Hold or Release Funds" form.

Overage Evaluation and Payment

Student accounts are reviewed on an ongoing basis for overages. If the overage occurs, it will be evaluated and paid after the student reaches the eighty percent point of the program.

MyComputerCareer is governed by the Department of Education, the states in which we do business and our accrediting body, amongst others. Our policies and procedures follow the guidelines set forth by each of these organizations. In the event the rules and regulations of our governing bodies prohibit MyComputerCareer from paying a credit balance or overage according to the time frames set forth above, the rules and regulations of that governing body will supersede those of MyComputerCareer.

Title IV Funds Return

Students who receive Title IV aid (Federal Pell, Federal SEOG, Federal Subsidized and/or Federal Unsubsidized Stafford loans and PLUS.) and withdraw from school are subject to the Return of Title IV aid regulations. (Federal law requires that a student must "earn" the aid that they receive.) When a student withdraws from school, the school is required to determine the amount "earned" using the Return of Title IV regulations. When calculating a R2T4 the department of education determines a student earns quarter credit hours when they have completed academic work to receive a passing grade in the course. This calculation is based on the percentage of the period completed and the pace, where necessary, at which the student is progressing. The percentage of the period completed is determined by dividing the number of calendar days completed in the payment period as of the student's last day of attendance by the total number of calendar days in the period unless the student is not on pace to complete the payment period within the expected timeframe. If the student is not on pace, the payment period will be lengthened based on the student's rate of progress. If the student completes more than 60% of the payment period, it is determined that all the aid has been earned. If a student completes 60% or less of the payment period, the earned and unearned portion will be calculated. The first Payment Period is complete once a student passes three courses (22.5 Academic Quarter Credits) for Certificate Programs. The second payment period starts the day after the first payment period. The Associate Degree period of obligation is based on each term.

1. The "unearned" portion of the institutional charges will be returned by the institution to the appropriate Title IV program. The institution will then bill the student for the amount of institutional charges that were returned in excess of the college's refund policy.
2. The "unearned" portion of the aid that was disbursed directly to the student will also be calculated. If applicable, the student will owe repayment to the Title IV programs. The student will receive an overpayment letter and will be given 45 days to make the repayment. The student will be eligible for further Title IV aid during the 45-day period but will become ineligible after the 45 days has passed. The student will remain ineligible until the funds are repaid or satisfactory payment arrangements have been made with the Department of Education.
3. Last day of verifiable attendance will be considered the withdrawal date for official or unofficial withdrawals.
    - Official Withdrawal – Formal notice of intent to WD in (writing, email, verbal) to the Lead Instructor or a Director of Education.
    - Unofficial Withdrawal – 14 consecutive days of no attendance.
4. The timeframe for the return of Title IV program funds is forty-five days from the Date of Determination (DOD) unless the State or other governing body in which the school is operating has a more stringent deadline.

The school will return Title IV funds to the programs from which the student received aid during the payment period as applicable, in the following order, up to the net amount disbursed from each source:

- Unsubsidized Direct Stafford loans
- Direct PLUS loans.
- Subsidized Direct Stafford loans.
- Federal Pell Grants for which a return of funds is required.

If a student started and qualified for a disbursement of **Pell**:

1. The funds can be disbursed without student authorization as per the "Treatment of Title IV Funds When Student Withdrawals" (R2T4) calculation and no later than 180 days of the DOD as a post withdrawal disbursement.
2. If an individual completed a FAFSA and clears Verification or a C Code, they can also become eligible for a post withdrawal disbursement or late disbursement of Pell (not direct loans) w/in 180 days of the DOD.

Any post-withdrawal disbursement of grant funds that is not credited to the student's account will be disbursed no later than 45 days after the date of determination that the student withdrew.

If a student started and qualified for a disbursement of **Direct Loan:**

1. The funds can be disbursed only after authorization from the borrower as per the "Treatment of Title IV Funds When a Student Withdrawals" (R2T4) calculation and no later than 180 days of the DOD.
2. In the unusual circumstance where a post withdrawal disbursement can be requested during the second payment period the disbursement must happen within 180 days of the students last date of attendance.

A student may be eligible for a **post-withdrawal disbursement** if, prior to withdrawing, the student earned more federal financial aid than was disbursed. If a student is eligible for a post-withdrawal disbursement for Title IV funds, it will be processed for the student and a refund will be issued within 14 days of the credit balance.

If the post-withdrawal disbursement includes loan funds, MyCC must get the student's permission before it can disburse the loan. Students may choose to decline some or all of the loan funds so that s/he does not incur additional debt. A notice will be sent out to the student, and the signed, original document must be returned to the School within 14 days.

MyComputerCareer may automatically use all or a portion of the post-withdrawal disbursement of grant funds for tuition and fees. However, the school needs the student's permission to use the post-withdrawal grant disbursement for all other school charges. If the student does not give his/her permission, the student will be offered the funds. However, it may be in the student's best interest to allow the school to keep the funds to reduce the student's debt at the school.

It is also important to understand that accepting a post-withdrawal disbursement of student loan funds will increase a student's overall student loan debt that must be repaid under the terms of the Master Promissory Note. Additionally, accepting the disbursement of grant funds will reduce the remaining amount of grant funds available to the student should the student continue his/her education at a later time.

Exit Counseling

Within 30 days of graduating or leaving school, Direct Loan borrowers must complete exit counseling. The Direct Loan Exit Counseling will explain your rights and responsibilities as a Direct Loan borrower and help with repayment information and options. Exit counseling is to be done at: https://studentloans.gov/myDirectLoan/index.action

Academic Calendar

The start dates for the programs at MyComputerCareer are dependent upon sufficient enrollment. Enrollment periods will begin approximately 6-8 weeks before the start date of class and end within one week after the start date of class. Program start dates occur approximately every 5 weeks. Enrollment in the IT ProBasic program will have start dates that occur on the same dates as the ITSA program. The table contains approximate CWP, ITSA, CSS, CSE and NACS enrollment terms for the 2024-2026 academic years.

ITSA - Monday Start		CSS - 30wk		CSE - 30wk		CWP - Online Day		CWP - Online Eve	
Start Date	End Date	Start Date	End Date	Start Date	End Date	Start Date	End Date	Start Date	End Date
7/1/2024	2/2/2025	7/2/2024	3/2/2025	7/29/2024	3/17/2025	11/13/2024	2/19/2025	1/29/2024	7/18/2024
8/5/2024	3/9/2025	8/6/2024	4/6/2025	9/2/2024	4/21/2025	12/13/2024	3/19/2025	2/27/2024	8/15/2024
9/9/2024	4/13/2025	9/10/2024	5/11/2025	10/7/2024	5/26/2025	1/22/2025	4/16/2025	3/26/2024	9/15/2024
10/14/2024	5/18/2025	10/15/2024	6/15/2025	11/11/2024	6/30/2025	2/20/2025	5/14/2025	4/23/2024	10/13/2024
11/18/2024	6/22/2025	11/19/2024	7/20/2025	12/16/2024	8/4/2025	3/20/2025	6/12/2025	5/21/2024	11/12/2024
12/30/2024	7/27/2025	12/31/2024	8/24/2025	1/27/2025	9/8/2025	4/17/2025	7/14/2025	6/20/2024	12/12/2024
2/3/2025	8/31/2025	2/4/2025	9/28/2025	3/3/2025	10/13/2025	5/15/2025	8/11/2025	7/19/2024	1/19/2025
3/10/2025	10/5/2025	3/11/2025	11/2/2025	4/7/2025	11/17/2025	6/13/2025	9/9/2025	8/16/2024	2/16/2025
4/14/2025	11/9/2025	4/15/2025	12/7/2025	5/12/2025	12/22/2025	7/15/2025	10/7/2025	9/16/2024	3/17/2025
5/19/2025	12/14/2025	5/20/2025	1/18/2026	6/16/2025	1/26/2026	9/10/2025	12/8/2025	10/15/2024	4/15/2025
6/23/2025	1/25/2026	6/24/2025	2/22/2026	7/21/2025	3/2/2026	10/8/2025	1/14/2026	11/13/2024	5/14/2025
7/28/2025	3/1/2026	7/29/2025	3/29/2026	8/25/2025	4/6/2026	11/6/2025	2/12/2026	12/13/2024	6/12/2025
9/1/2025	4/5/2026	9/2/2025	5/3/2026	9/29/2025	5/11/2026	12/9/2026	3/15/2026	1/22/2025	7/14/2025
10/6/2025	5/10/2026	10/7/2025	6/7/2026	11/3/2025	6/15/2026	1/15/2026	4/12/2026	2/20/2025	8/11/2025
11/10/2025	6/14/2026	11/11/2025	7/12/2026	12/8/2025	7/20/2026	2/13/2026	5/10/2026	3/20/2025	9/9/2025
12/15/2025	7/19/2026	12/16/2025	8/16/2025	1/12/2026	8/24/2026	3/16/2026	6/8/2026	4/17/2025	10/7/2025
1/26/2026	8/23/2026	1/27/2026	9/20/2026	2/16/2026	9/28/2026	4/13/2026	7/7/2026	5/15/2025	11/5/2025
3/2/2026	9/27/2026	3/3/2026	10/25/2026	3/23/2026	11/2/2026	NACS - 85wk		6/13/2025	12/8/2025
4/6/2026	11/1/2026	4/7/2026	11/29/2026	4/27/2026	12/7/2026	Start Date	End Date	7/15/2025	1/14/2026
5/11/2026	12/6/2026	5/12/2026	1/18/2027	CSE - 22.5 Transfer		4/23/2024	12/10/2025	8/12/2025	2/12/2026
6/15/2026	1/17/2027	CSS - 22.5 Transfer		Start Date	End Date	5/28/2024	1/14/2026	9/10/2025	3/15/2026
ITSA - Tuesday Start		Start Date	End Date	9/17/2024	1/6/2025	7/2/2024	2/18/2026	10/8/2025	3/9/2026
Start Date	End Date	9/2/2024	12/15/2024	10/22/2024	2/10/2025	8/6/2024	3/25/2026	11/6/2025	4/6/2026
7/2/2024	2/3/2025	10/7/2024	1/26/2025	11/26/2024	3/17/2025	9/10/2024	4/29/2026	12/9/2025	5/4/2026
8/6/2024	3/10/2025	11/11/2024	3/2/2025	1/7/2025	4/21/2025	10/15/2024	6/3/2026	1/15/2026	6/2/2026
9/10/2024	4/14/2025	12/16/2024	4/6/2025	2/11/2025	5/26/2025	11/19/2024	7/8/2026	2/17/2026	6/30/2026
10/15/2024	5/19/2025	1/27/2025	5/11/2025	3/18/2025	6/30/2025	12/31/2024	8/19/2026	3/10/2026	7/21/2026
11/19/2024	6/23/2025	3/3/2025	6/15/2025	4/22/2025	8/4/2025	2/4/2025	9/23/2026	4/7/2026	8/18/2026
12/31/2024	7/28/2025	4/7/2025	7/20/2025	5/27/2025	9/8/2025	3/11/2025	10/28/2026	5/5/2026	9/16/2026
2/4/2025	9/1/2025	5/12/2025	8/24/2025	7/1/2025	10/13/2025	4/29/2025	12/16/2026	6/3/2026	10/15/2026
3/11/2025	10/6/2025	6/16/2025	9/28/2025	8/5/2025	11/17/2025	6/3/2025	1/20/2027	7/1/2026	11/16/2026
4/15/2025	11/10/2025	7/21/2025	11/2/2025	9/9/2025	12/22/2025	7/8/2025	2/24/2027		
5/20/2025	12/15/2025	8/25/2025	12/7/2025	10/14/2025	2/1/2026	8/12/2025	3/31/2027		
6/24/2025	1/26/2026	9/29/2025	1/18/2026	11/18/2025	3/8/2026	9/16/2025	5/5/2027		
7/29/2025	3/2/2026	11/3/2025	2/22/2026	12/29/2025	4/12/2026				
9/2/2025	4/6/2026	12/8/2025	3/29/2026	2/2/2026	5/17/2026				
10/7/2025	5/11/2026	1/19/2026	5/3/2026	3/9/2026	6/21/2026				
11/11/2025	6/15/2026	2/23/2026	6/7/2026	4/13/2026	7/26/2026				
12/16/2025	7/20/2026	3/30/2026	7/12/2026	5/18/2026	8/30/2026				
1/27/2026	8/24/2026	5/4/2026	8/16/2026	6/22/2026	10/4/2026				
3/3/2026	9/28/2026	6/8/2026	9/20/2026	7/27/2026	11/8/2026				
4/7/2026	11/2/2026	7/13/2026	10/25/2026	8/31/2026	12/13/2026				
5/12/2026	12/7/2026	8/17/2026	11/29/2026						
6/16/2026	1/18/2027	9/21/2026	1/10/2027						

School Holidays

MyComputerCareer will be closed and not hold classes on the following holidays: New Year's Day, Memorial Day, Fourth of July, Labor Day, Thanksgiving Day and for a week around Christmas.

Attendance Policy

Attendance is critical to the success of students who attend the programs at MyComputerCareer. Absences can prevent students from succeeding in class and hinder their preparation for starting a career in the computer industry. A maximum of 20% of absences is permitted by the school towards the attendance completion requirement. MyComputerCareer will record all attendance for students. A student who misses multiple classes in a course due to an extreme circumstance, may request to make-up the class time with his/her Instructor or Lead Instructor. A student must complete 80% of their scheduled clock hours in each course in order to avoid receiving a failing grade for the course. Students who receive a failing grade for the course will be required to repeat the course as discussed in the "Repeating Courses" section below. Students who fail two courses in the first payment period or more than two courses in the program are subject to Academic Termination. Payment period is defined as the successful completion of 22.5 Quarter Credit Hours (3 courses).

Absences

Students are expected to attend each class session on time and participate actively in class. Students are also expected to complete the required number of laboratory hours each week. If a student will be absent from class, they are expected

to inform the instructor by email or phone prior to the start of class. The accumulation of absences exceeding 20% of scheduled clock hours in any course will prevent the student from receiving credit for the course and cause it to be failed. Students who do not receive credit for a course will be required to repeat the course as discussed in the "Repeating Courses" section below. Students who fail two courses in the first payment period or more than two courses in the program are subject to Academic Termination. **Students with no attendance for 14 consecutive calendar days will be dismissed from their program and withdrawn for violation of the attendance policy. CWP students will be dismissed after 2 consecutive days of no attendance.** Dismissed students must submit an appeal to their Lead Instructor within 5 business days of termination. Approval of appeal is at the discretion of the Appeals Committee.

Make-up Work

Students who need to complete missed assignments and receive additional review of topics missed in class should make arrangements with their Lead Instructor or Instructor. Students must complete the required minimum number of hours, assignments and/or make-up work by the end date of each course. A student who misses multiple classes in a course due to an extreme circumstance, may request to make-up the class time with his/her Instructor or Lead Instructor. The Lead Instructor will create the academic plan with the student to use during make-up time. An Academic Recovery Plan form will be used for this purpose. Once the student agrees to the plan, the Lead Instructor will approve the make-up time. If the student does not agree, the make-up time will not be approved. Students who do not complete the minimum required hours and/or assignments by the end of each course will receive a failing grade for that course. Students who receive a failing grade in a course will be required to repeat the course as discussed in the "Repeating Courses" section below. Students who fail two courses in the first payment period or more than two courses in the program are subject to Academic Termination.

Tardiness & Early Departures

Students are expected to be on time for all class sessions, exams, material review sessions, and so forth. Tardiness is defined as any time missed after the start of class. Early Departure is defined as any time remaining prior to the end of class. Tardiness and early departures are recorded on a real-time basis with students logging in immediately upon arrival and immediately upon departure. Consistent tardiness can adversely affect the learning environment. Excessive tardiness or early departures can result in not meeting the required hours for the training program. Students falling below these minimum requirements may earn a failing grade for the course, may be required to repeat the course, and may be subject to Academic Termination if they fail two courses in the first payment period or more than two courses in the program.

Repeating Courses

To progress timely through the program, and to meet graduation requirements, MyComputerCareer students are expected to achieve a passing grade and minimum attendance requirements by the end date of each course.

If a student does not achieve a minimum passing grade of 60%, and a minimum of 80% attendance, by the end date of a course, the student will not receive credit for the course. The student must repeat the failed course and achieve a minimum passing grade of 60%, and a minimum of 80% attendance, to successfully pass the course. A cumulative GPA of 70% and, for each course, attendance of 80% must be achieved to meet graduation standards.

MyComputerCareer will allow a student to repeat a failed course at no additional tuition cost to the student. A student will not be eligible for additional federal financial assistance for the repeat courses.

Upon successfully passing the repeated course, and achieving required attendance in the repeated course, the grade earned in the repeated course will replace the grade in the failed course in order to determine the cumulative GPA. All credits in the repeated course and in the failed course will be included as credits attempted.

The student must repeat the failed course when it is scheduled by the school administration. The student may take a different course in their program prior to repeating the failed course. Effort will be made by MyComputerCareer to align the repeat course with the student's current schedule, but due to limited availability of seats in repeat classes, the repeat course may be scheduled for a different time/day that the student's original schedule. If for any reason the student does not repeat the failed course, then the student will be subject to Academic Termination from the program.

A student will be Academically Terminated if the student fails two courses in the first payment period. As a reminder, a payment period is defined as the successful completion of 22.5 Quarter Credit Hours (3 courses). If the student fails three courses in the program, the student will be Academically Terminated. No Appeal will be available to students under either of these circumstances. A student may repeat a course that they have already passed in two limited circumstances: (1) a single round-out course during the student's final term, if required, for students receiving military benefits; or (2) a course to replace a course preventing the student from achieving a cumulative GPA of 70% to graduate.

Should the student pass their individual courses but not achieve the required cumulative Program GPA of 70%, the student will not be allowed to graduate and may appeal their Did Not Graduate status. In order to graduate, MyComputerCareer will allow the student to retake courses they have already passed, as determined and scheduled by the school administration, to achieve the minimum passing course grade needed to meet the cumulative Program GPA of 70%. A minimum of 80% attendance must be achieved in the repeat course. The repeat course's grade will replace the originally passed course's grade. All credits in the repeated course and in the prior course will be included as credits attempted. No additional tuition cost will be charged to the student for this repeat course.

All required courses in the program must be completed and passed, and the minimum cumulative Program GPA achieved, within the maximum time frame of the published length of the program. Retakes will only be allowed when it is mathematically possible to reach graduation standards.

Students enrolled at the Raleigh Main Campus or any of its branches as identified on the inside cover of this catalog may have their retake course taught by an Instructor from the Raleigh Main campus or any of the Raleigh branch campuses, in the unlikely event that it is not available when needed in order to complete training for graduation from the home campus.

Repeating Courses - VA Students Impact

In conjunction with the course repeat policy, VA students are unable to repeat courses using benefits where they have successfully passed the course (60% course grade, 80% attendance) with VA funding. As a result, when courses are repeated but the original course has met the minimum requirements, the course may not be certified for VA funding or certification. When a course is being repeated and the original course was not passed, the course will be certified with no additional tuition and fees. The impact to the housing allowance and eligibility usage will be at the discretion of the VA. Whenever possible the repeated course will be scheduled to minimize the financial impact. However, if a financial impact occurs as a result of the repeating course, the impacted student will be notified by a school certifying official accordingly.

Leave of Absence

A leave of absence (LOA) may be permitted when a student faces a temporary problem such as military deployment, accident, death in the family, change in teaching methodology or other emergency. Any student who seeks a leave of absence must submit the signed, dated request in writing and specify a reason to the Lead Instructor prior to the beginning date of the LOA, unless unforeseen circumstances prevent a student from doing so. An email may be accepted as deemed necessary by the Director of Education or Program Chair. Corroborating documentation may be required. The granting, denial, and duration of a leave of absence will be done on a case-by-case basis at the sole discretion of MyComputerCareer. In order for a leave of absence to be granted, MyComputerCareer must have a reasonable expectation that the student will return to the program at the end of the leave of absence. Students returning from an LOA will enter at the appropriate place during the next available class as determined by the Director of Education or Program Chair. If a student fails to reenter the class at the end of the leave of absence, the student will be academically terminated from the program. Students have five business days to appeal termination. The leave of absence(s) is limited to 180 calendar days in any 12-month period or one-half the published program length, whichever is shorter. An approved LOA may be extended for an additional period of time provided that the extension request meets all of the above requirements.

Intent to Return

If a course is unavailable due to unexpected schedule changes making it necessary for a student to interrupt his/her training, MyComputerCareer may permit a student to remain enrolled until the course is available. This is common when a student needs to repeat a course previously failed in order to meet graduation requirements, but the course is not immediately available. Courses are typically available every five to seven weeks depending on the program. The following requirements must be met for approval:

1. The student must request and complete the Intent to Return form available from the school.
2. A School Official must approve and sign the Intent to Return request.
3. Intent to Return may be approved only if the school can determine there is reasonable assurance that the student will return on the scheduled returned date, which must be no later than 60 calendar days from the date the student ceases attendance.
4. Upon approval of and during the Intent to Return period, the school does not assess the student any additional institutional charges, the student's need may not increase, and the student is not eligible for any additional Federal Student Aid.
5. The school must provide an explanation to the student, prior to granting the Intent to Return, regarding the effects that the student's failure to return from an Intent to Return may have on the student's loan repayment terms, including the expiration of the student's grace period.
6. Students must return on the class start date of the course needed for graduation.
7. Existing financial obligations, where applicable, remain in effect during an Intent to Return period.
8. Students who fail to return to class on their scheduled Intent to Return date are dropped from the program.

9. An Intent to Return may be extended if a written request is received on or prior to the scheduled return date, but the return date must be no later than 60 calendar days from the date the student originally ceased attendance.

Grades & Graduation Standards

The chart to the right is the grading scale based on the percentage of points earned over the length of a program or course.

% of Total Points Earned	Letter Grade	GPA
90-100	A	4.0
80-89	B	3.0
70-79	C	2.0
60-69	D	1.0
59 or below	F	0.0
Temporary Leave of Absence	L	n/a

The final grade will be comprised of multiple components, each critical to the success of the student. Refer to the course syllabus for each course breakdown. The table to the right shows the common breakdown of the final grade for vocational programs: (Note: Avocational courses will only consist of tests as the criteria for the total grade)

Criteria	% of Total Grade
Final Exam	40%
Post Assessments	30%
Graded Labs	20%
Homework Assignments	10%

A student must achieve the following to graduate from a program at MyComputerCareer:

1. Completion of all credit hours in the program
2. Cumulative grade percentage of 70% or higher (2.0 GPA)
3. Minimum GPA of 60% is required for individual courses. (not applicable for Avocational courses)
4. Completion of 80% of the scheduled clock hours in each course.
5. Completion of the graduation requirements within the maximum program length, which is 143% of the published length of the program. (not applicable for Avocational courses)

All graduates will receive a Certificate of Completion or Diploma, based on program of enrollment.

Transcript Request

Students may request a copy of their academic transcript at any time by visiting the campus, calling the campus directly or emailing the Site Coordinator. There is no transcript release fee at this time.

Satisfactory Academic Progress

Progress Standards for all students in Credit Hour Programs:

A. Quantitative progress is based upon the successful completion of credit hours. A student must have earned 70 percent of the attempted credit hours.
B. Qualitative progress is based upon the cumulative grade point average. The minimum cumulative GPA required is 70 percent.
C. Students must be progressing at a rate which would allow them to complete their program within 143 percent of the scheduled weeks for the program.

Evaluation Points:

All Certificate Programs are one academic year in length. SAP will be evaluated at the scheduled program midpoint, the program end date and the program's maximum time frame (or 143 percent). For the Associate's Degree Program, SAP will be evaluated at the end of each payment period and the program's maximum time frame (or 143 percent). At each evaluation period, both quantitative and qualitative progress will be measured, which specifically includes the cumulative GPA and pace as outlined above in the "Progress Standards for Credit Hour Programs" description. Students that do not meet SAP standards at midpoint or lab end date may be Academically Terminated as defined below.

All students are able to access their On-Track Progress Check (OTPC), via their time clock. The OTPC provides a snapshot of their academic and attendance status throughout the program towards meeting graduation requirements. Attendance is updated daily, while their GPA and credits earned vs attempted is updated at the end of each course.

All Quarter Credit Hour programs are less than one year in length. Eligible Title IV disbursements will be made at the beginning of each program and again at the program midpoint. SAP will be evaluated at the scheduled program midpoint, the program end date and the program maximum time frame (or 143% date). At each evaluation period both quantitative and qualitative progress will be measured as outlined above in the "Progress Standards for Credit Hour Programs" description. Students that do not meet SAP standards at the scheduled midpoint or at the scheduled end date will be Academically Terminated as defined below.

Academic Termination and Financial Aid Probation:

Students not meeting the SAP standards at the scheduled evaluation point will be notified via email of their Academic Termination. When a student loses Title IV eligibility and is academically terminated because he or she fails to make Satisfactory Academic Progress, the student may submit an Appeal as described in the next section. If an Appeal is approved, the student will be placed on Financial Aid Probation. When the student is placed on Financial Aid Probation, an

Academic Plan will be developed and provided to the student. This Academic Plan must allow the student to meet SAP standards by the Maximum Time Frame of the program. The student's Satisfactory Academic Progress will be evaluated at the end of the next payment period, as is required of a student on Financial Aid Probation status, to determine if the student is meeting the minimum standards of SAP or if the student is meeting the requirements of the Academic Plan. The student is eligible to receive Title IV aid while on Financial Aid Probation and the Academic Plan, as long as the student continues to meet the minimum standards of SAP or is meeting the requirements of the Academic Plan. Students not meeting the minimum requirements following the payment period when the student is on Financial Aid Probation will no longer be eligible for Title IV aid and will be terminated unless a subsequent appeal is submitted and granted. If the student previously appealed on the basis of one circumstance and intends to appeal again based on the same circumstance, the student must provide information about what has changed to permit the student to make satisfactory academic progress at the next evaluation. The Cyber Warrior Program is not Title IV eligible.

Appeal Process:

Students academically terminated from MyComputerCareer will be notified via email of their dismissal. The student may submit a written Appeal (email is an accepted form of written communication) to the Director of Education or Program Chair within five business days of the dismissal notification. Students who fail two courses in the first payment period or who fail more than two courses in the entire program will not be eligible to appeal their termination.

Appeals are considered for mitigating circumstances defined as: documented student illness/injury which is an emergency or severe in nature, death of an immediate relative, personal tragedy or natural disaster, called to active military duty and/or other mitigating circumstances that are not everyday occurrences of life and are beyond your control. The Appeal must include a definitive statement from the student defining the mitigating circumstances as to why s/he failed to meet SAP standards and what has changed in the student's situation that will allow him/her to meet SAP standards at the next SAP evaluation. Documentation may be required with the Appeal.

Upon a successful appeal, the student will be placed on Financial Aid Probation and given an Academic Plan. The Academic Plan will clearly identify a path for the student to successfully complete the program within the maximum timeframe allowed.

The Appeals Committee, composed of the Director of Education and one or two members of the executive leadership as needed, will examine all Appeals. The approval or denial of the Appeal is at the sole discretion of the Appeals Committee. The student will be sent the Appeals Committee's decision within five business days of the Director of Education or Program Chair's receipt of the appeal. The decision of the Appeals Committee is final. The withdrawal calculation for students whose appeal is denied will be based upon their last day of attendance.

Transfer Students:

Students awarded transfer credits will have their enrollment term adjusted based on the number of Quarter Credit Hours remaining in the program. Transfer credits will be counted toward the maximum timeframe and will count as credits attempted and credits earned in the quantitative evaluation of SAP.

Course Repeats:

Repeat courses in the classroom training environment must be discussed with the instructor for the class and the Director of Education or Program Chair. Students who repeat courses will not be eligible for additional federal or military financial assistance for the repeat courses. See the **Repeating Courses** section for further details.

Incomplete Courses, Remedial Courses, Course Withdrawals, and Internal Program Transfer:

If a student does not successfully complete a course by the end of the course's scheduled end date, MyComputerCareer counts the credits in the course as attempted credit hours toward the student's Quantitative progress, but not as earned credit hours.

MyComputerCareer generally does not allow individual course withdrawals, nor does it offer remedial programs.

All periods of enrollment count towards the determination of SAP including periods when a student does not receive Title IV aid. Additionally, when a student pursues another program at MyComputerCareer, only those credits for the courses that apply toward the second program count in the calculation of SAP for the second program.

Attendance & Progress Standards for VA Students in North Carolina

VA students will be evaluated at the end of each course. If a student failed to meet standards (80% attendance, 70% grade average) during that course, s/he will be placed on probation for the following course. At the end of the course of

probation, if the student continued to fail to meet standards (80% attendance, 70% academic standards), s/he will be terminated. Summary: 1 month below standards; 1 month on probation; then termination.

Students wishing to appeal this action due to mitigating circumstances must do so in writing within five business days. Please refer to the **Appeal Process**.

VA Re-entry Policy: updated 10/29/2018
Once a student is terminated, the following actions will be accomplished for re-entry:

- Student must be terminated for a period of 60 days before consideration for re-entry,
- Student will submit a new application for admission,
- The Appeals Committee will evaluate student's written request and status; determine the student has sufficient ability and potential to warrant a 2nd entry,
- Director of Education will provide the student
  (1) letter of re-entry,
  (2) contract for re-entry specifying hours of pursuit,
  (3) notification that student is on VA probation for one course after re-entry
- If the student has not obtained standards of progress at the end of the course, s/he will be terminated and will not receive future consideration for re-entry.

Attendance & Progress Standards for VA Students enrolled in Ohio and Indiana

VA students must meet all academic standards of progress for MyCC including, but not limited to the Satisfactory Academic Progress policy. In addition, VA funded students will be evaluated at the end of each course (five weeks for the 30-wk. program, seven weeks for the 42-wk. program) to maintain eligibility for GI Bill® certification.

- Attendance of 80% of scheduled clock-hours or higher for that course.
- GPA of a 2.0 or higher for that course.

Students not meeting this requirement at the end of any course will be placed on VA Academic Probation. Students on VA Academic Probation will have until the end of the next course to meet these standards. When the above standards are met the student will be removed from VA Academic Probation. Failure to meet these standards by the end of the probationary period will result in an Academic Termination. Students wishing to appeal this action due to mitigating circumstances must do so in writing within five business days. Please refer to the **appeal process**.

Attendance & Progress Standards for VA Students enrolled in Texas

Unsatisfactory attendance, is reported to the Department of Veteran Affairs on VA form 22-199b and may result in a reduction and/or loss of BAH and possible termination of Enrollment Certification. For Resident Enrollments this includes an absence of five consecutive business days; and for Hybrid or Full IDL enrollments this includes five days based on your enrollment class schedule.

VA students must also meet all academic standards of progress for MyCC including, but not limited to the Satisfactory Academic Progress policy. VA funded students will be evaluated at the end of each course (five weeks for the 30-wk. program, seven weeks for the 42-wk. program) to maintain eligibility for GI Bill® certification.

At the end of each course VA funded students must meet the following non-cumulative standards:

- GPA of 70% or higher for that course.
- Attendance of 80% of scheduled clock-hours or higher for that course.

Students not meeting this requirement at the end of any course will be placed on VA Academic Probation Students on VA Academic Probation will have until the end of the next course to meet these standards. When the above standards are met the student will be removed from VA Academic Probation. Failure to meet these standards by the end of the probationary period will result in an Academic Termination. Students wishing to appeal this action due to mitigating circumstances must do so in writing within five business days. Please refer to the appeal process.

Cancellation and Refund Policies

ACCET

a. If an applicant is rejected for enrollment or the program is canceled prior to the start of the program a full refund will be made. If an applicant cancels prior to the start of scheduled classes or never attends class (no-show), the institution will issue a full refund of tuition and fees.
b. Refund amounts must be based on a student's last date of attendance (LDA). When determining the number of weeks completed by the student, the institution may consider a partial week the same as if a whole week were completed, provided the student was present at least one day during the scheduled week.
c. During the first week of classes, tuition charges withheld must not exceed 10 percent (10%) of the stated tuition up to a maximum of $1,000.
d. After the first week and through fifty percent (50%) of the period of financial obligation, tuition charges retained must not exceed a pro rata portion of tuition for the training period completed, plus ten percent (10%) of the unearned tuition for the period of training that was not completed, up to a maximum of $1,000.
e. After fifty percent (50%) of the period of financial obligation is completed, the institution may retain the full tuition.

State of North Carolina

The tuition refund to which students are entitled as a result of withdrawal or dismissal is governed by regulations of the State of North Carolina General Statutes and Administrative Code and by the Accrediting Council for Continuing Education and Training. MyComputerCareer will base refunds on whichever policy is most beneficial to the student based upon the current regulations from both entities. The student has the right to cancel this agreement at any time. If the school rejects the student, one hundred percent (100%) tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund one hundred percent (100%) tuition and fees paid by the student. A no-show is defined as any cancellation of enrollment prior to the Lab Start Date. A one hundred percent (100%) refund of tuition and fees will be made to all enrolled students determined to be a no-show. Refunds for books, tools, or other supplies will be handled separately from refund of tuition and fees. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased and the student starts the program, no refund will be made.

Refund computations will be based on scheduled course time of class attendance through the last date of attendance. Leaves of absence, suspensions, and school holidays will not be counted as part of the scheduled class attendance. The effective date of termination for refund purposes will be the last day of attendance. The institution may retain an administrative fee associated with withdrawal or termination not to exceed $100. When determining the number of weeks completed by the student, the institution will consider a partial week the same as if a whole week were completed, provided the student was present at least one day during the scheduled week. A seventy-five percent (75%) refund, excluding any disclosed non-refundable fees, if the student officially withdraws or is officially withdrawn by the school on or before reaching twenty-five percent (25%) of the total instructional hours of the program in which the student is enrolled. After the 25% mark and through fifty percent (50%) of the period of financial obligation, tuition charges retained will not exceed a prorated portion of tuition for the training period completed, plus ten percent (10%) of the unearned tuition for the period of training that was not completed, up to a maximum of $1,000. After fifty percent (50%) of the period of financial obligation is completed, the school may retain the full tuition.

A request for withdraw can be delivered or sent to the training center in writing, via email or can be verbally conferred to the Lead Instructor or a Director of Education. If an applicant never attends class all refunds will be paid within 45 calendar days from the first scheduled day of class or the date of the withdrawal request, whichever is earlier. For students that attend a class, all refunds due will be paid within 45 calendar days from the documented date of determination. The date of determination is the date the student gives written or verbal notice of withdrawal to the Lead Instructor, a Director of Education or the date the institution terminates the student by applying MyComputerCareer's attendance, conduct or SAP policy.

State of Texas

The tuition refund, to which students are entitled as a result of withdrawal or dismissal, is governed by regulations of the State of Texas Education Code and ACCET accreditation standards. MyComputerCareer will base refunds on whichever policy is most beneficial to the student based upon the current regulations from both entities. Currently, the State of Texas Education Code for refunds is consistently more lenient towards the student. The student has the right to cancel this agreement at any time. If the school rejects the student, all tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund all tuition and fees paid by the student. A no-show is defined as any cancellation of enrollment prior to the Lab Start Date. A full refund of tuition and fees will be made

to all enrolled students determined to be a no-show. Refunds for books, tools, or other supplies will be handled separately from refund of tuition and fees for students who start the program and have taken possession of the items. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased and the student starts the program, no refund will be made.

Refunds for books, tools, or other supplies will be handled separately from refund of tuition and fees. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased, no refund will be made.

Tuition Refunds

1. Refund computations will be based on scheduled course time of class attendance through the last date of attendance. LOAs, suspensions, and school holidays will not be counted as part of the scheduled class attendance.
2. The effective date of termination for refund purposes will be the last day of attendance.
3. A full refund will be made to any student who cancels the enrollment contract within 72 hours (until midnight of the third day excluding Saturdays, Sundays and legal holidays) after the enrollment contract is signed and a tour of the facilities and inspection of the equipment is made by the prospective student or who cancels within the student's first three scheduled class days
4. If tuition and fees are collected in advance of entrance, and if after expiration of the 72 hour cancellation privilege the student does not enter school, not more than $100 in nonrefundable administrative fees shall be retained by the school for the entire residence program or synchronous distance education course.
5. If a student withdraws or is otherwise terminated, the school or college may retain not more than $100 in nonrefundable administrative fees for the entire program.
6. The minimum refund of the remaining tuition and fees will be the pro rata portion of tuition, fees, and other charges that the number of hours remaining in the portion of the program (term for Associates Degree) for which the student has been charged after the effective date of termination bears to the total number of hours in the portion of the course or program for which the student has been charged, except that a student may not collect a refund if the student has completed 75 percent or more of the total number of hours in the portion of the program for which the student has been charged on the effective date of termination.
7. A no-show is defined as any cancelation of enrollment prior to the Lab Start Date.
8. A student who withdraws for a reason unrelated to the student's academic status after the 75 percent completion mark and requests a grade at the time of withdrawal shall be given a grade of "incomplete" and permitted to re-enroll in the course or program during the 12-month period following the date the student withdrew without payment of additional tuition for that portion of the course or program.
9. A full refund of all tuition and fees is due and refundable in each of the following cases:
   (1) An enrollee is not accepted by the school;
   (2) If the course of instruction is discontinued by the school and this prevents the student from completing the course;
   (3) A no-show; or
   (4) If the student's enrollment was procured as a result of any misrepresentation in advertising, promotional materials of the school, or representations by the owner or representatives of the school.

   A full or partial refund may also be due in other circumstances of program deficiencies or violations of requirements for career schools and colleges.

Refund Policy For Students Called To Active Military Service.

10. A student of the school or college who withdraws from the school or college as a result of the student being called to active duty in a military service of the United States or the Texas National Guard may elect one of the following options for each program in which the student is enrolled:
    (a) if tuition and fees are collected in advance of the withdrawal, a pro rata refund of any tuition, fees, or other charges paid by the student for the program and a cancellation of any unpaid tuition, fees, or other charges owed by the student for the portion of the program the student does not complete following withdrawal;
    (b) a grade of incomplete with the designation "withdrawn-military" for the courses in the program, other than courses for which the student has previously received a grade on the student's transcript, and the right to re-enroll in the program, or a substantially equivalent program if that program is no longer available, not later than the first anniversary of the date the student is discharged from active military duty without payment of additional tuition, fees, or other charges for the program other than any previously unpaid balance of the original tuition, fees, and charges for books for the program; or
    (c) the assignment of an appropriate final grade or credit for the courses in the program, but only if the instructor or instructors of the program determine that the student has:
       (1) satisfactorily completed at least 90 percent of the required coursework for the program; and
       (2) demonstrated sufficient mastery of the program material to receive credit for completing the program.

11. The payment of refunds will be totally completed such that the refund instrument has been negotiated or credited into the proper account(s), within 45 days after the effective date of termination.

A request for withdraw can be delivered or sent to the training center in writing, via email or can be verbally conferred to the Lead Instructor or a Director of Education. If an applicant never attends class all refunds will be paid within 45 calendar days from the first scheduled day of class or the date of the withdrawal request, whichever is earlier. For students that attend a class, all refunds due will be paid within 45 calendar days from the documented date of determination. The date of determination is the date the student gives written or verbal notice of withdrawal to the Lead Instructor, a Director of Education or the date the institution terminates the student by applying MyComputerCareer's attendance, conduct or SAP policy.

State of Indiana

Indianapolis Campus

The tuition refund, to which students are entitled as a result of withdrawal or dismissal, is governed by regulations of the Indiana Administrative Code and the ACCET accreditation standards. MyComputerCareer will base refunds on whichever policy is most beneficial to the student based upon the current regulations from both entities. The student has the right to cancel this agreement at any time. If the school rejects the student, all tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund all tuition and fees paid by the student. A full refund will be made to any student who cancels the enrollment contract within 6 calendar days after the enrollment contract is signed. A no-show is defined as any cancellation of enrollment prior to the Lab Start Date. A full refund of tuition and fees will be made to all enrolled students determined to be a no-show. Refunds for books, tools, or other supplies will be handled separately from refund of tuition and fees for students who start the program and have taken possession of the items. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased and the student starts the program, no refund will be made.

The student has the right to cancel this agreement at any time. If the school rejects the student, all tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund all tuition and fees paid by the student. The student may cancel within six calendar days from the date the enrollment agreement was signed and will receive a full refund of all money paid to the school or its representatives. After six days from the day the agreement was signed, but before the school term starts, the student will receive a full refund of all tuition and fees paid. After the school term has started the refund policy listed below will apply. The last day of verifiable attendance by the student will be considered as the withdrawal date for refund calculations. Upon cancellation all monies due to the student will be refunded within thirty-one days.

a. A student is entitled to a full refund if one (1) or more of the following criteria are met:
    1. The student cancels the enrollment agreement or enrollment application within six (6) business days after signing.
    2. The student does not meet the postsecondary proprietary educational institution's minimum admission requirements.
    3. The student's enrollment was procured as a result of a misrepresentation in the written materials utilized by the postsecondary proprietary educational institution.
    4. If the student has not visited the postsecondary educational institution prior to enrollment, and, upon touring the institution or attending the regularly scheduled orientation/classes, the student withdrew from the program within three (3) days.
b. A student withdrawing from an instructional program, after starting the instructional program at a postsecondary proprietary institution and attending one (1) week or less, is entitled to a refund of ninety percent (90%) of the cost of the financial obligation, less an application/enrollment fee of ten percent (10%) of the total tuition, not to exceed one hundred dollars ($100).
c. A student withdrawing from an instructional program, after attending more than one (1) week but equal to or less than twenty-five percent (25%) of the duration of the instructional program, is entitled to a refund of seventy- five percent (75%) of the cost of the financial obligation, less an application/enrollment fee of ten percent (10%) of the total tuition, not to exceed one hundred dollars ($100).
d. A student withdrawing from an instructional program, after attending more than twenty-five percent (25%) but equal to or less than fifty percent (50%) of the duration of the instructional program, is entitled to a refund of fifty percent (50%) of the cost of the financial obligation, less an application/enrollment fee of ten percent (10%) of the total tuition, not to exceed one hundred dollars ($100).
e. A student withdrawing from an instructional program, after attending more than fifty percent (50%) but equal to or less than sixty percent (60%) of the duration of the instructional program, is entitled to a refund of forty percent (40%)

of the cost of the financial obligation, less an application/enrollment fee of ten percent (10%) of the total tuition, not to exceed one hundred dollars ($100).

f. A student withdrawing from an institutional program, after attending more than sixty percent (60%) of the duration of the instructional program, is not entitled to a refund.

State of Ohio

Columbus Campus

The tuition refund, to which students are entitled as a result of withdrawal or dismissal, is governed by regulations of the State Board of Career Colleges and Schools (OH Administrative Rule 3332-1-10) and the ACCET accreditation standards. MyComputerCareer will base refunds on whichever policy is most beneficial to the student based upon the current regulations from both entities. The student has the right to cancel this agreement at any time. If the school rejects the student, all tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund all tuition and fees paid by the student. A full refund will be made to any student who cancels the enrollment contract within 5 calendar days after the enrollment contract is signed. A no-show is defined as any cancellation of enrollment prior to the Lab Start Date. A full refund of tuition and fees will be made to all enrolled students determined to be a no-show. Refunds for books, tools, or other supplies will be handled separately from refund of tuition and fees for students who start the program and have taken possession of the items. The student will not be required to purchase instructional supplies, books and tools until such time as these materials are required. Once these materials are purchased and the student starts the program, refunds will be made in accordance with OAC 3332-1-10.1.

The student has the right to cancel this agreement at any time. If the school rejects the student, all tuition and fees will be refunded. If the institution cancels a program subsequent to a student's enrollment, the institution will refund all tuition and fees paid by the student. The student may cancel within five calendar days from the date the enrollment agreement was signed and will receive a full refund of all money paid to the school or its representatives. After five days from the day the agreement was signed, but before the school term starts, the student will receive a full refund of all tuition and fees paid. After the school term has started the refund policy listed below will apply. The last day of verifiable attendance by the student will be considered as the withdrawal date for refund calculations. Upon cancellation all monies due to the student will be refunded within thirty days.

a. A student who starts class and withdraws during the first full calendar week of the academic term shall be obligated for 25 percent of the tuition and refundable fees for that academic term plus the registration fee.
b. A student who withdraws during the second full calendar week of the academic term shall be obligated for fifty per cent of the tuition and refundable fees for that academic term plus the registration fee.
c. A student who withdraws during the third full calendar week of the academic term shall be obligated for seventy-five per cent of the tuition and refundable fees for that academic term plus the registration fee.
d. A student who officially withdraws beginning with the fourth full calendar week of the academic term will not be entitled to a refund of any portion of the tuition or refundable fees.

A request for withdraw can be sent to the training center in writing, via email or can be verbally conferred to the Lead Instructor or a Director of Education. If an applicant never attends class all refunds will be paid within 30 calendar days from the first scheduled day of class or the date of the withdrawal request, whichever is earlier. For students that attend a class, all refunds due will be paid within 30 calendar days from the documented date of determination. The date of determination is the date the student gives written or verbal notice of withdrawal to the Lead Instructor, a Director of Education or the date the institution terminates the student by applying MyComputerCareer's attendance, conduct or SAP policy.

3332-1-10.1 Refunds for books, fees and supplies.

(a) In the event that a student withdraws or is dismissed from school, all efforts will be made to refund pre-paid amounts for books, fees and supplies except for those items determined to fall within the preview of paragraphs (B)(1) and (B)(2) of this rule.
(b) Charges for required purchase of books, fees and supplies can be non-refundable if the student has consumed or used the books, fees and/or supplies. Consumption of books, fees and supplies shall be defined as:
    1. Items that were special ordered for a particular student and cannot be used by or sold to another student; or,
    2. Items that were returned in a condition that prevents them from being used by or sold to new students.
    3. Individually documented non-refundable fees for goods or services provided by third party vendors.
(c) Items or services not delivered to the student cannot be considered consumed except for those items covered by paragraph (B) (1) of this rule.
(d) A record of the refund determination for books, fees and supplies shall be kept in the student's record.

California Regulation:

(Residents of California ~ Columbus and Indianapolis Full IDL only)

The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the Fund STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition. You are not eligible for protection from the STRF and you are not required to pay the STRF assessment if you are not a California resident, or are not enrolled in a residency program. It is important that you keep copies of your enrollment agreement, financial aid documents, receipts, or any other information that documents the amount paid to the school. Questions regarding the STRF may be directed to the Bureau for Private Postsecondary Education, 1747 North Market, Suite 225 Sacramento, CA 95834, (916) 431-6959 or (888) 370-7589.

To be eligible for STRF, you must be a California resident or enrolled in a residency program, prepaid tuition, paid or deemed to have paid the STRF assessment, and suffered an economic loss as a result of any of the following:

1. The institution, a location of the institution, or an educational program offered by the institution was closed or discontinued, and you did not choose to participate in a teach-out plan approved by the Bureau or did not complete a chosen teach-out plan approved by the Bureau.
2. You were enrolled at an institution or a location of the institution within the 120 day period before the closure of the institution or location of the institution, or were enrolled in an educational program within the 120 day period before the program was discontinued.
3. You were enrolled at an institution or a location of the institution more than 120 days before the closure of the institution or location of the institution, in an educational program offered by the institution as to which the Bureau determined there was a significant decline in the quality or value of the program more than 120 days before closure.
4. The institution has been ordered to pay a refund by the Bureau but has failed to do so.
5. The institution has failed to pay or reimburse loan proceeds under a federal student loan program as required by law, or has failed to pay or reimburse proceeds received by the institution in excess of tuition and other costs.
6. You have been awarded restitution, a refund, or other monetary award by an arbitrator or court, based on a violation of this chapter by an institution or representative of an institution, but have been unable to collect the award from the institution.
7. You sought legal counsel that resulted in the cancellation of one or more of your student loans and have an invoice for services rendered and evidence of the cancellation of the student loan or loans.

To qualify for STRF reimbursement, the application must be received within four years from the date of the action or event that made the student eligible for recovery from STRF. A student whose loan is revived by a loan holder or debt collector after a period of non-collection may, at any time, file a written application for recovery from STRF for the debt that would have otherwise been eligible for recovery. If it has been more than four years since the action or event that made the student eligible, the student must have filed a written application for recovery within the original four year period, unless the period has been extended by another act of law. However, no claim can be paid to any student without a social security number or a taxpayer identification number."

5-CCR 76120. STRF Assessment Fee. (a) As of 4/1/2024, each qualifying institution shall collect an assessment of $0.00 per one thousand dollars of institutional charges, rounded to the nearest thousand dollars, from each student in an educational program who is a California resident or is enrolled in a residency program. This fee is included in the registration fee for each Columbus program.

Dismissal from a Program

Students are expected to conduct themselves in a professional manner and to act, speak, and show respect to others as in a business environment. MyComputerCareer reserves the right to dismiss students for activities detrimental to themselves, other students, and the school. Reasons for dismissal include, but are not limited to, the following:

- Any Behavior that negatively affects the learning environment.
- Unlawful possession, use, or distribution of illicit drugs and alcohol.
- Providing false information required during the admissions process.
- Violation of the terms and conditions of the Enrollment Agreement.
- Violating the Copyright Infringement Policy
- Falsifying student records.
- Not meeting Satisfactory Academic Progress.
- Failing two courses in the first payment period or failing three courses in the program.
- Failure to attend for 14 consecutive calendar days. (2 days for CWP students)
- Nonpayment of any student loan.

If a student is dismissed from the program and wants to re-enter the same program where they left off, they must go through the enrollment process within 180 days of withdraw date. After 180 days would be considered a new enrollment with transfer credit, where applicable. The Admission process is outlined on pages 5-6 depending on your State. Approval for reenrollment is at the sole discretion of MyCC.

Grievance Procedure

All student complaints should be communicated to the Director of Education or Program Chair. Students that have addressed their concern to the Director of Education or Program Chair and have not reached their desired outcome, or have an issue directly related to the Director of Education or Program Chair are encouraged to write a letter to Tony, founder and CEO of MyComputerCareer, by going to http://info.mycomputercareer.com/dear-tony. The student will be contacted, and an attempt will be made to resolve the complaint internally to the satisfaction of the student, within reasonable discretion. Students are encouraged to go through this internal complaint process as a first attempt to resolve any complaints.

If the complaint cannot be resolved, the student will be referred to the higher governing authority listed below:

Ohio students may contact the State Board of Career Colleges and Schools at 30 East Broad St. Suite 2481 Columbus, OH 43215-3414, Phone 614-466-2752, t oll free at 877-275-4219 or email bpsr@scr.state.oh.us.

Residents of **California** enrolled in distance education through Columbus, OH may file a complaint at https://www.bppe.ca.gov/enforcement/complaint.shtml. A complaint may be filed using the online complaint submission link or by downloading a complaint form and mailing it to: Bureau for Private Post-Secondary Education, PO Box 980818, West Sacramento, VA 95798-0818.

Indiana students may file a formal complaint at the Indiana Commission for Higher Education located at 101 West Ohio Street Suite 300 Indianapolis, IN 46204. Phone 317-464-4400 or Email - Complaints@che.in.gov. https://www.in.gov/che/student-complaints/. Residents of **California** enrolled in distance education through Indianapolis, IN may file a complaint at https://www.bppe.ca.gov/enforcement/complaint.shtml. A complaint may be filed using the online complaint submission link or by downloading a complaint form and mailing it to: Bureau for Private Post-Secondary Education, PO Box 980818, West Sacramento, VA 95798-0818.

Texas - School Number: Arlington: S4925 * Dallas: S3367 * Houston: S3692 * Sugar Land S5686 * Raleigh IDL S5898 Students may file a formal complaint with TWC, who provides our Certificate of Approval and approves all of MyComputerCareer's programs, by completing the Student Complaint Form and following the instructions in the following link : http://www.twc.state.tx.us/files/jobseekers/csc-401a-student-complaint-form-twc.pdf. Additional information on filing a complaint can be found at http://www.texasworkforce.org/careerschoolstudents. Complaint forms can be sent to: TWC Career Schools and Colleges, 101 East 15th Street, Room 226T, Austin, Texas 78778-0001. Phone: (512) 936-3100.

North Carolina students may file a formal complaint by completing the Student Complaint Form and following the instructions in the following link: https://studentcomplaints.northcarolina.edu/form.

In addition, students can submit complaints to **ACCET** by following the complaint procedure posted in each campus or by clicking on the following link that contains their contact information: ACCET Complaint Procedure. ACCET's address and phone number are as follows: 1722 N Street, NW Washington, DC 20036 Telephone: 202-955-1113.

All Campuses and state-by-state complaint procedures for NC-SARA and non-SARA schools can also be found on our website at - https://www.mycomputercareer.edu/additional-disclosure-statements/

Agreement to Arbitrate

As a condition of enrollment, Student and MyComputerCareer agree to resolve through binding and mandatory arbitration any dispute, claim, controversy, cause of action, lawsuit, or proceeding (including, but not limited to, any statutory, tort, contract or equity claim) between Student and MyComputerCareer or any current or former employee(s) of MyComputerCareer (collectively, the "Parties") that arises, arose, or has arisen out of, or is or was in any way related to, this Enrollment Agreement, the subject matter of this Enrollment Agreement, or Student's enrollment, attendance, or educational experience at MyComputerCareer (individually and collectively, a "Dispute"). The Parties are encouraged to make an initial attempt, in good faith, to resolve the Dispute through MyComputerCareer's student complaint process or other informal means. If the Dispute is not resolved pursuant to MyComputerCareer's student complaint process or other informal means, then the Dispute will be resolved by binding arbitration between the Parties.

1. Explanation of Arbitration. Arbitration is the referral of a Dispute to an impartial person (an arbitrator) for a final and binding determination of the Dispute. In agreeing to binding and mandatory arbitration, the Parties voluntarily give up certain rights, including the right to pursue a Dispute in court, the right to a trial by a judge or jury, rights to appeal, and other rights that may be available in a court, such as broader discovery rights. As provided by this arbitration provision, the Parties also give up the right to bring or participate in any class action, collective action, private attorney

general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others.

2. Arbitration Procedures.
   (a) The arbitration will be administered by the American Arbitration Association ("AAA") or, in the event the AAA declines or is unable to administer the arbitration, by an arbitration forum or arbitrator that the Parties mutually agree upon. If, after making a reasonable effort, the Parties are unable to agree upon an arbitration forum or arbitrator, a court having proper jurisdiction will appoint an arbitration forum or arbitrator. The arbitration will be conducted in accordance with the AAA's Consumer Arbitration Rules, or the appropriate rules of any alternative arbitration forum selected by the Parties or appointed by a court, except as modified by this arbitration provision. The AAA's Consumer Arbitration Rules and other information regarding the AAA's arbitration procedures are available from the AAA, which can be contacted by mail at 120 Broadway, Floor 21, New York, New York 10271, by telephone at 212-716-5800, or through its website at www.adr.org.
   (b) Any Dispute shall be heard by a single arbitrator who is an attorney. As a condition of appointment, the arbitrator shall follow all applicable substantive laws (except as otherwise provided in this arbitration provision), shall agree to the terms of this arbitration provision, and shall lack authority not to enforce the terms of this arbitration provision. The arbitrator shall have the exclusive authority to determine and adjudicate any issue relating to the existence, formation, validity, enforceability, applicability, or interpretation of this Enrollment Agreement and this arbitration provision, provided, however, that a court shall have exclusive authority to enforce the Class Action Prohibition. The arbitrator's decision shall be accompanied by a reasoned opinion from which there shall be no appeal.
   (c) The place of arbitration shall be the location (city and state) of the campus where the Dispute arose ("Campus"). Judgment on the arbitral award may be entered exclusively in the location of the Campus. The law of the state of the Campus shall apply.
   (d) The Parties shall each bear their own attorney's fees, costs, and expenses, except that the costs of arbitration, as set forth in the AAA Consumer Arbitration Rules, shall be determined by the AAA Consumer Arbitration Rules.
   (e) This arbitration provision governs if there is a conflict with the rules of the arbitral forum.
3. Class Action Prohibition. The scope of the arbitration shall be limited to the Dispute between the Parties. The Parties expressly waive all rights to bring any class action, collective action, private attorney general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others. The arbitrator shall have no authority or jurisdiction to compel, hear, or permit any class action, collective action, private attorney general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others. By way of illustration and not limitation, neither Student nor MyComputerCareer can bring a class action against each other or participate in a class action against the other, whether as a named class representative or an absent or putative class member.
4. Federal Arbitration Act. The Parties agree that this Arbitration Agreement involves interstate commerce and that the enforceability of this Arbitration Agreement shall be governed, both procedurally and substantively, by the Federal Arbitration Act, 9 U.S.C. §§ 1-9.
5. Severability. If the Class Action Prohibition is found to be illegal or unenforceable as to all or some parts of a Dispute, then those parts will not be arbitrated but will be resolved in court, with the balance of the Dispute resolved through arbitration. If any other part of this arbitration provision is found to be illegal or unenforceable, then that part will be severed; however, the remaining parts shall still apply and shall be interpreted to as nearly as possible achieve the original intent of this arbitration provision.
6. Small Claims Lawsuits Permitted. Notwithstanding anything to the contrary, this arbitration provision does not prevent the Parties from filing a lawsuit in any small claims court of competent jurisdiction.
7. Modifications to Arbitration Agreement. As required by 34 C.F.R. § 685.300(e) and (f), regulations promulgated by the United States Department of Education in 2022, we agree to the following modifications of this arbitration agreement, but only to the extent and so long as the regulations requiring the modifications remain in effect. To the extent the regulation is declared invalid by a court of competent jurisdiction or is rescinded by the United States Department of Education, the modification associated with the invalidated or rescinded regulation shall immediately become null and void:
8. Modification Required by 34 C.F.R. § 685.300(e). We agree that this agreement cannot be used to stop you from being part of a class action lawsuit in court. You may file a class action lawsuit in court, or you may be a member of a class action lawsuit even if you do not file it. This provision applies only to class action claims concerning our acts or omissions regarding the making of the Direct Loan or our provision of educational services for which the Direct Loan was obtained. We agree that the court has exclusive jurisdiction to decide whether a claim asserted in the lawsuit is a claim regarding the making of the Federal Direct Loan or the provision of educational services for which the loan was obtained.
9. Modification Required by 34 C.F.R. § 685.300(f). We agree that neither we nor anyone else will use this agreement to stop you from bringing a lawsuit concerning our acts or omissions regarding the making of the Federal Direct Loan or

the provision by us of educational services for which the Federal Direct Loan was obtained. You may file a lawsuit for such a claim, or you may be a member of a class action lawsuit for such a claim even if you do not file it. This provision does not apply to lawsuits concerning other claims. We agree that only the court is to decide whether a claim asserted in the lawsuit is a claim regarding the making of the Federal Direct Loan or the provision of educational services for which the loan was obtained.

10. Modification Required by NC-SARA Membership, effective 7/1/2024. MyComputerCareer participates in NC-SARA and is not permitted to enforce this Arbitration Agreement on students enrolled under NC-SARA provisions. This Arbitration Agreement is not applied when a student files a complaint or dispute that falls within the scope of the NC-SARA Policy Manual.

Software Piracy, Copyright Laws, and Internet Use

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject those in violation to civil and criminal liabilities.

Potential Civil and Criminal Sanctions for Copyright Infringement:

- In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed.
- For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.
- Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the website of the U.S. Copyright Office at www.copyright.gov.

MyComputerCareer strictly prohibits the piracy of software and the violation of piracy and copyright laws and reserves the right to dismiss students from the program who are found to be using the equipment to illegally copy software or other copyrighted materials for their own gain. No student should attempt to copy, make available, or distribute copies of copyrighted material. Inappropriate conduct and violations for willfully violating this policy will be reviewed and addressed by Site Coordinator based on the campus in which the student is enrolled. Academic consequences for willfully violating copyright laws include, but are not limited to: 1.Receiving a grade of 0 for a test or assignment where the violation took place. 2. Receiving a grade of 0 in the course where the violation took place. 3. Dismissed from the Program.

Students will have access to the Internet for educational purposes only. Surfing the Internet or using any Internet based application during class is strictly prohibited, including all social networking sites and all web based messenger services, unless specifically required by labs and the instructor.

Student recording of classroom lectures, discussions, and/or activities is not permitted unless a student has an approved accommodation prior to starting their full program. It is expected that all students regularly and actively participate in their scheduled classroom sessions in order to best engage with the learning material, openly explore with their co-student key concepts, and have their questions answered for understanding in real-time.

Confidentiality of Student Records

The policy of MyCC is to comply with the Family Educational Rights and Privacy Act (FERPA) and, in so doing, protect the confidentiality of personally identifiable educational records of students and former students. The student has the following rights: the right to inspect and review his/her education records within 45 days of the day the school receives a request for access; the right to request an amendment of his/her education records that the student believes are inaccurate or misleading; the right to consent to disclosures of personal identifiable information (pii) contained in his/her education records except to the extent that FERPA authorizes disclosure without consent; and the right to file a complaint with the U.S. Department of Education concerning alleged failures by MyCC to comply with the requirements of FERPA. A health and safety exception permits the disclosure of pii from a student's record to appropriate parties if knowledge of the information is necessary to protect the health or safety of the student or other individuals from an immediate threat.

Career and Student Services

MyComputerCareer provides lifetime career services to students currently enrolled in or graduates of any Vocational program at MyComputerCareer. Career services at MyComputerCareer consist of but are not limited to:

(a) Resume preparation assistance
(b) Cover Letter preparation assistance
(c) Interview preparation
(d) Job referrals
(e) Career counseling
(f) Application Assistance
(g) Tutoring (See Campus Hours section)
(h) Refresher Courses (see Alumni Services Dept for details and limited timeframe)

Students are encouraged to meet with their Career Services Director often to discuss the status of their career search and their training stage and certification level. The Career Services Director will serve as a liaison between the student and employer and continually works to build and improve relationships with local employers in the area. MyComputerCareer cannot by law guarantee a job upon completion of the student's program.

Background checks are a standard part of the hiring process for many employers. If you have a criminal history it will impact your job search. MyComputerCareer cannot define that impact for you.

Student counseling resources for personal growth, financial and legal issues and Mental Health Resources are available in their Learning Management System. Topics include, but not limited to, Stress, Anxiety, Depression, Finances, Trauma, Relationships, parenting, Drug & Alcohol, etc.

* MyComputerCareer offers Graduates past their Maximum Time Frame period the opportunity to continue preparing to take select IT certification exams for certifications that they did not earn during their active program. Please contact the Alumni Services Department for additional information and enrollment requirements for the Boot Camp and certification refresher content opportunities.

Visitors

The Site Coordinator must approve all visitors to our campus. Visitors are not permitted in our classrooms and are to remain in the lobby area. Bringing children to campus during class or flextime is prohibited.

Instructional Equipment

Technology is essential to your success! Whether you are taking classes online or on-campus you will need a laptop. All MyComputerCareer Information Technology courses do not require you to purchase any textbooks. All course materials are available electronically. MyComputerCareer provides an option to opt-in and purchase a laptop for an additional $550.00 for the ITPB, ITSA, CSS, CSE and the Associate Degree Programs. This is not a required fee as we understand that you may already have a personal laptop and would like to avoid charges that are not necessary based on your current technological needs. During the enrollment process, you will have the opportunity to opt-in to purchase a non-refundable laptop, which will increase the total cost by an additional $550.00. If you already have a laptop, it should meet the minimum requirements outlined below. Students who opt-in to receive the laptop will also have at least the minimum spec requirements below:

- Webcam
- 13-inch or larger screen preferred
- At least 100 GB of available storage
- Intel i3, AMD Ryzen 3, or better
- Microphone
- Windows 10 or higher
- 8 GB of RAM
- Wi-Fi adapter (802.11n or better)

We reevaluate laptop configurations frequently to keep our students up to date with the latest technology. If you plan to purchase a laptop on your own with the above minimum requirements you will find many affordable options at any of the following stores or on their website: www.bestbuy.com, www.newegg.com, www.microcenter.com, www.amazon.com.

Certification Conditions

There are no courses or programs offered by MyComputerCareer requiring state licensure or state certification.

All students should review the EC-Council Code of Ethics in the CEH Handbook before enrolling any program offering EC Council Certifications (CSS, CSE, Associates NACS) found here - https://cert.eccouncil.org/images/doc/CEH-Handbook-v4.0.pdf. The infringement of any exam policies, rules, NDA, certification agreement or the involvement in misdemeanor that may harm the integrity and image of EC-Council certification program, may result in the candidate's temporary or permanent ban, at EC-Council's discretion, from taking any future EC-Council certification exams, revocation or decertification of current certifications. Such infringements include but are not limited to:

1. The publication of any exam contents or parts with any person without a prior written approval from EC-Council.
2. The recreation, imitation, or replication of any exam content through any means including memory recalling whether free or paid through any media including Web forums, instant messaging, study guides, etc.
3. Harnessing any materials or devices not explicitly authorized by EC-Council during the exam.
4. Taking out any materials that hold any exam contents outside the exam room, using for example, scratch paper, notebook, etc.
5. The impersonation of a candidate.

6. Meddling with the exam equipment in an unauthorized way.
7. Giving or being receptive of any assistance unauthorized by EC-Council.
8. Acting in au uncivil, disturbing, mobbish, or unprofessional manner that may disregard or disrespect other candidates or exam officials during the exam.
9. Communicating by whatever verbal or non-verbal means with other candidates in the exam room.
10. Not adhering to EC-Council Exam Retake Policy and other candidate agreements.
11. Not adhering to EC-Council Code of Ethics.
12. Felony conviction in the court of law.

Drug and Alcohol Prevention Policy, Tobacco Use, Clery Act, VAWA

Tobacco use of any kind (e-cig, chewing tobacco, etc.) is prohibited on campus. All employees and students are forbidden to use, possess, transfer or sell illegal drugs on company premises. Violators will be subject to disciplinary action, including immediate discharge for employees and expulsion for students. All employees and students are forbidden to use, possess or be under the influence of alcohol on company premises. Violators will be subject to disciplinary action that may include immediate discharge for employees and expulsion for students. All employees and students are prohibited from . being under the influence of any drug on company premises. Any off-duty employee or student who is arrested for possession, use, being under the influence of or selling illegal drugs will be suspended pending the outcome of the judicial proceedings. The employee or student will be discharged or dismissed if subsequently convicted of a drug-related crime. Illegal use, possession or distribution of drugs is subject to criminal legal sanctions under local, state and federal law. Additional information on this topic as well as detailed information on the Clery Act, Title IX, VAWA and Campus Crime and Safety can be found on our website at https://www.mycomputercareer.edu/additional-disclosure-statements/

Student Right-to-know Act

MyComputerCareer, acting in compliance with the Student Right to Know Act, is happy to provide information on the graduation rates of our cohorts of full-time, first-time, certificate-seeking undergraduates, that have received financial aid.

You can find this information along with details on other general information such as student diversity at the College Navigator link located here: https://www.mycomputercareer.edu/additional-disclosure-statements/.

Vocational Program Offerings

Program Updates:

MyComputerCareer will change the curriculum of a program as new technologies and certifications become available within the industry. These changes are for the benefit of the student to ensure students are receiving relevant training. All applicable agencies such as the State and Accreditor will approve any course changes before they are implemented. MyComputerCareer will not be obligated to update the program as new technologies emerge within the industry.

Definitions:

1. Lecture hours are defined by ACCET as “instructional hours consisting of theory or new principles”.
2. Lab Hours are defined by ACCET as “Instructional hours consisting of supervised student practice of a previously introduced theory/principle during which practical skills are developed and reinforced”.
3. Accreditation (ACCET) Placement Definitions
4. Academic Definition of a Credit: Vocational program lengths are measured in Quarter Credit Hours using the Carnegie clock-to-credit conversion. One (1) Quarter Credit Hour is equivalent to ten (10) Lecture Hours. One (1) Quarter Credit Hour is also equivalent to twenty (20) Lab Hours.
    a. Effective 7/1/2021, VA Enrollments will be certified under Academic Quarter Credit Hours for all IHL Institutions/Programs.
5. Academic Year Definition – 45 QCH’s for 30 Weeks and/or 45 QCH’s for 42 Weeks
6. Full Interactive Distance Learning (IDL) = 100% distance education
7. Hybrid Interactive Distance Learning (IDL) = 50% distance education and 50% on-campus resident training
8. Payment Period is defined as the successful completion of 22.5 AQCHs (3 courses).

Enrollment Prerequisites – CSS & CSE

Cyber Security Specialist:

1. Graduate of the ITSA Program, or
2. Two years of IT Industry work experience, or
3. One year of IT Industry work with a min. of an Associate's Degree, or
4. Proof of an Active A+ Certification

Cyber Security Engineer:

1. Graduate of the ITSA, CWP or CSS Program, or
2. Three years of IT Industry work experience, or
3. Two years of IT Industry work experience with a min. of an Associate's Degree, or
4. Proof of an Active Security+ Certification

An updated resume is required to show proof of work experience. Military work experience in computer technology is applicable for work experience. Proof of Degree and/or Active Certification is required for criteria 3 and 4.

Avocational Courses

Avocational, Professional Development courses, also known as a "Seminar" in Texas, are designed for individuals who want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field who want to stay current with IT skills and certification information to meet the demands of their profession. Career Services and Job Placement assistance are not available for Avocational courses.

Attendance & Completion Requirements

1-5 week Avocational Courses

1. Must attend 70% of the total course clock hours to earn a Certificate of Completion

12-week Avocational Courses

1. Students with no attendance or assignments completed within 21 consecutive calendar days will be withdrawn
2. Attend a minimum of two Certification Mastery Course modules by the end of the course
3. Attendance in a repeat module will count towards course completion
4. Complete a minimum of two Learning Lab assignments

24 and 30-week Avocational Courses

1. Students with no attendance or assignments completed within 21 consecutive calendar days will be withdrawn
2. Attend a minimum of four modules by the end of the course
3. Attendance in a repeat module will count towards course completion
4. Complete a minimum of two Learning Lab assignments

Raleigh Programs and Campus Staff

5511 Capital Center Dr. Suite 500 Raleigh, NC 27606 ~ 919-301-0951

Campus Faculty & Staff

Todd Duhamel – Senior Director of Education
Josh Davies – Director of Education
Open – Asst. Director of Admission
Eric Bryant – Admissions Advisor
Nicholas Davis – Admissions Advisor
Katheryn McHale – Admissions Advisor
Paul Totten – Admissions Advisor
Aimee Bowman – Asst. Dir. Of Career Services
Richard Saltares – Asst. Dir. Of Career Services
Shareef Ivey – Career Services Team Lead Advisor
Antuan Snead –Career Services Team Lead Advisor
Joseph Tally – Career Services Team Lead Advisor
Andre Jackson – Career Services Specialist
Cheryl Lafer – Career Services Specialist
Jazz Lyons – Career Services Specialist
Jessica Celestin – Career Services Specialist
Antuan Snead – Career Services Specialist
Arinn Williamson – Career Services Specialist
Bridgette Colbert-Paulin – Career Services Specialist
Derrick Daniel – Career Services Specialist
Joseph Tailly – Career Services Specialist
Staci Barfield – Career Services Specialist
Jayme Cherry – Office Administrator
Kay Fogle – VA Specialist
Jerry Bastien – Lead Instructor
Ray Downing – Lead Instructor
Jim Atria – Lead Instructor
Chris Reid – Lead Instructor
Michael Viola – Lead Instructor
Andrew Collins – Lead Instructor
Terrance Robinson – Lead Instructor
Charles Ponton – Lead Instructor
Robert Pacheco – Lead Instructor
Jill Schaumloeffel – Lead Instructor
Jerry Carrillo – Lead Instructor
Charles Carter – Lead Instructor
John Early – Lead Instructor
Delores Hudson – Lead Instructor
Russ Munisteri – Lead Instructor
Bernard Bullington – Lead Instructor
Candace Kiser – Lead Instructor
Kristina Wong – Lead Instructor
Scott Stromberg – Lead Instructor

Information Technology Security and Administration (ITSA)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives

The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- Systems Administrators
- PC Repair Technicians
- Level I, II and III Help Desk Support
- Technical consultants

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,613.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,048.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student's skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19 or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:

The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Teaching Methodology: Resident, Hybrid IDL, or Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00	Term One Curriculum[1]	$2,726
Tuition term one	$9,135.50	Term Three CEH Curriculum[1]	$1,072
Tuition term two	$9,135.50	Term Four Curriculum[1]	$2,435
Tuition term three	$11,024	Term Four CFR Curriculum[1]	$650
Tuition term four	$11,024	Term Five Gen Ed. Software[1]	$300
Tuition term five	$2,485	Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:

ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is

for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States’ political history and improve students’ understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic

business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to recognize threats and manage risks in hardening an organization's security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course
Tuition: $495 Enrollment Term: 12 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course
Tuition: $595 Enrollment Term: 24 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course
Tuition: $595 Enrollment Term: 30 weeks
Course Clock Hours: 36 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:
A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Charlotte Programs and Campus Staff

3701 Arco Corporate Dr. Suite 115 Charlotte, NC 28273 ~ 704-302-1031

Campus Faculty & Staff

Nate Ferkovich – Assistant Director of Admissions (Site Coordinator)
Reuben Brown – Admissions Advisor
Nica Henderson – Admissions Advisor
Raelene Burke – Admissions Advisor
Ashley Brown – Office Administrator
Lena Foote – Office Administrator
Kay Fogle – VA Specialist
Richard Saltares – Asst. Dir. Career Services
Caroleen Harris – Career Services Specialist
Carlos Lewis – Lead Instructor
Felicia Bellamy – PT Instructor

Information Technology Security and Administration (ITSA)

Learning Methodology: Resident, Hybrid IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives

The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- PC Repair Technicians
- Technical consultants
- Systems Administrators
- Level I, II and III Help Desk Support

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites – CSS & CSE on page 26
Academic QCHs: 45, Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,613.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs

Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,048.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student's skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students

will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident, Hybrid IDL, or Full IDL
QCHs: 112.5,
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Curriculum[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Curriculum[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:
ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems,

laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security

enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States' political history and improve students' understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization’s security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to recognize threats and manage risks in hardening an organization’s security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity

intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist

Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course

Tuition: $495 Enrollment Term: 12 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course

Tuition: $595 Enrollment Term: 24 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course

Tuition: $595 Enrollment Term: 30 weeks
Course Clock Hours: 36 hours Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:

A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Arlington Programs and Campus Staff

1701 E. Lamar Blvd. Suite 250 Arlington, TX 76006 ~ 817-210-6308

Campus Faculty & Staff

Jessica Toney – Sr. Assistant Director of Admissions (Site Coordinator)
PT Instructor – Ray Genova
Lisa Clough – Career Services Specialist
Kenneth Graves – Sr. Admissions Advisor
Kaitlyn Smith – Admissions Advisor
I'Keliha Williams – Admission Advisor
David Dean– Admissions Advisor
Kay Fogle – VA Specialist
Angela Pointer – Sr. Office Administrator
J.Patrick Hines – Lead Instructor
Marvin Thompson – Lead Instructor
Dan Ward – Lead Instructor
Chris Reid – Lead Instructor
Brian Edwards – Lead Instructor
Alpesh Patel – Lead Instructor
Josh Renihan – Lead Instructor
Terrance Robinson – Lead Instructor
Kristin Wong – Lead Instructor
Scott Stromberg – Lead Instructor
Mike Kalka – Lead Instructor
Russ Munisteri – Lead Instructor
Jill Schaumloeffel – Lead Instructor

IT ProBasic Program

Learning Methodology: Resident, Hybrid IDL or Full IDL
Academic QCHs: 22.5,
Clock Hours: 360
Enrollment Term: 15 or 21weeks
Award Attainment: Certificate

Program Cost	$	10,549.50
Tuition	$	9,135.50
Curriculum[1]	$	1,314.00
Registration Fee[1]	$	100.00

[1] These items are non-refundable once the student starts and issued to the student

The ITPB Program consists of three courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance and networking. The coursework and practice tests prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals and Microsoft Azure AI Fundamentals. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Vocational Objectives:

The objective of this program is to provide the technical skills and knowledge identified in the course descriptions below along with the professional soft skills needed to start and maintain a career in the IT Industry. Job opportunities exist within all levels of the economy from government employment, employment with Fortune 100 and 500 companies, and small businesses. Opportunities exist in all types of settings for these types of positions such as:

- Level I, II and III Help Desk Support
- PC Repair Technicians
- Technical Support Engineers
- Technical Consultants

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Information Technology Security and Administration (ITSA)

Learning Methodology: Hybrid IDL, or Full IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives

The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- PC Repair Technicians
- Technical consultants
- Systems Administrators
- Level I, II and III Help Desk Support

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to

core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45, Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,613.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5

Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,048.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student's skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated

with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident, Hybrid IDL, and Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Curriculum[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Curriculum[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:
ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems,

laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security

enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States' political history and improve students' understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization’s security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to recognize threats and manage risks in hardening an organization’s security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity

intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist

Tuition: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course

Tuition: $495
Enrollment Term: 12 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 24 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 30 weeks
Course Clock Hours: 36 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:

A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Dallas Programs and Campus Staff

12225 Greenville Ave. Suite 500 Dallas, TX 75243 ~ 214-646-3973

Campus Faculty & Staff

Mishonta Gentry – Assistant Director of Admissions (Site Coordinator)
Courteney Powell – PT Instructor
Margaret Kimani – PT Lab Assistant
Vanecia Alexander – Admissions Advisor
Trezuer Butler – Admissions Advisor
Charkesechia Nedd – Admissions Advisor
Sondra Parramore – Admissions Advisor
Rhonda Pope – Admissions Advisor
Brian Wirta – Career Services Specialist
Kay Fogle – VA Specialist
Sherette Robinson – Office Administrator
Derrick Austin – Lead Instructor
Michael Weekes – Lead Instructor
Mike Viola – Lead Instructor
Marvin Thompson – Lead Instructor
Mohamed Elbashir – Lead Instructor
Russ Munisteri – Lead Instructor
Chris Reid – Lead Instructor
Andrew Collins – Lead Instructor
Jill Schaumloeffel – Lead Instructor

IT ProBasic Program

Learning Methodology: Resident, Hybrid IDL or Full IDL
Academic QCHs: 22.5,
Clock Hours: 360
Enrollment Term: 15 or 21 weeks
Award Attainment: Certificate

Program Cost	$	10,549.50
Tuition	$	9,135.50
Curriculum[1]	$	1,314.00
Registration Fee[1]	$	100.00

[1] These items are non-refundable once the student starts and issued to the student

The ITPB Program consists of three courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance and networking. The coursework and practice tests prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals and Microsoft Azure AI Fundamentals. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Vocational Objectives:

The objective of this program is to provide the technical skills and knowledge identified in the course descriptions below along with the professional soft skills needed to start and maintain a career in the IT Industry. Job opportunities exist within all levels of the economy from government employment, employment with Fortune 100 and 500 companies, and small businesses. Opportunities exist in all types of settings for these types of positions such as:

- Level I, II and III Help Desk Support
- PC Repair Technicians
- Technical Support Engineers
- Technical Consultants

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Information Technology Security and Administration (ITSA)

Learning Methodology: Hybrid IDL or Full IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives

The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- PC Repair Technicians
- Technical consultants
- Systems Administrators
- Level I, II and III Help Desk Support

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to

core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,613.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,048.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student’s skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students

will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of

Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Teaching Methodology: Resident, Hybrid IDL, and Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Curriculum[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Curriculum[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:

ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of

endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States' political history and improve students' understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490
Course Clock Hours: 40 or 60 hours
Enrollment Term: 1-5 weeks
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490
Course Clock Hours: 40 or 60 hours
Enrollment Term: 1-5 weeks
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder

Tuition: $3,640
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization’s security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner

Tuition: $3,640
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to recognize threats and manage risks in hardening an organization’s security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials

Tuition: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst
Tuition: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist
Tuition: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course
Tuition: $495
Enrollment Term: 12 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course
Tuition: $595
Enrollment Term: 24 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course
Tuition: $595
Enrollment Term: 30 weeks
Course Clock Hours: 36 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:
A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495
CompTIA CySA+ Test Prep Package
Tuition: $495
CompTIA CASP+ Test Prep Package
Tuition: $645
CISCO CCNA Test Prep Package
Tuition: $495
A+ Essentials 1 Certification Test Prep Package
Tuition: $495
CISCO CyberOps Certification Test Prep Package
Tuition: $495
CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645
Network+ Essentials Certification Test Prep Package
Tuition: $495
EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645
A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Houston Programs and Campus Staff

12225 Greenville Ave. Suite 500 Dallas, TX 75243 ~ 214-646-3973

Campus Faculty & Staff

Valory Hemphill – Assistant Director of Admissions (Site Coordinator)
Will Brown – Admissions Advisor
Purvis Bowman – Admissions Advisor
Jade Sanusi - Admissions Advisor
Manuel Arreola - Admissions Advisor
Kay Fogle – VA Specialist
Montanya Charles – Career Services Specialist
Will Mobley – Career Services Specialist
Marty Mulsow – Lead Instructor
Gonazlo Regalado – Lead Instructor
Leos Segura – Lead Instructor
Rehan Ahmed – Lead Instructor
Deborah Edwards – Office Administrator

IT ProBasic Program

Learning Methodology: Resident, Hybrid IDL or Full IDL
Academic QCHs: 22.5
Clock Hours: 360
Enrollment Term: 15 or 21 weeks
Award Attainment: Certificate

Program Cost	$	10,549.50
Tuition	$	9,135.50
Curriculum[1]	$	1,314.00
Registration Fee[1]	$	100.00

[1] These items are non-refundable once the student starts and issued to the student

The ITPB Program consists of three courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance and networking. The coursework and practice tests prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals and Microsoft Azure AI Fundamentals. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Vocational Objectives:

The objective of this program is to provide the technical skills and knowledge identified in the course descriptions below along with the professional soft skills needed to start and maintain a career in the IT Industry. Job opportunities exist within all levels of the economy from government employment, employment with Fortune 100 and 500 companies, and small businesses. Opportunities exist in all types of settings for these types of positions such as:

- Level I, II and III Help Desk Support
- PC Repair Technicians
- Technical Support Engineers
- Technical Consultants

Course Sequence and Descriptions:

Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Information Technology Security and Administration (ITSA)

Learning Methodology: Resident, Hybrid IDL or Full IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives
The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- Systems Administrators
- PC Repair Technicians
- Level I, II and III Help Desk Support
- Technical consultants

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent

Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident, Hybrid IDL, and Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Curriculum[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Curriculum[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:

ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network

infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States’ political history and improve students’ understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the

United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to recognize threats and manage risks in hardening an organization's security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course

Tuition: $495 | Enrollment Term: 12 weeks
Course Clock Hours: 18 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 24 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 30 weeks
Course Clock Hours: 36 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:

A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Sugar Land Programs and Campus Staff

14141 SW Freeway Suite 1010 Sugar Land, TX 77478 ~ Phone – 832-939-3980

Campus Faculty & Staff

Joel Holt – Assistant Director of Admissions (Site Coordinator)
Joseph Jones – Admissions Advisor
Melinda Franco – Admissions Advisor
Leonard Wright – Career Services Specialist
Kay Fogle – VA Specialist
Tariq Salih - Lead Instructor
Assad Jumshyd – Instructor
Leos Segura – Lead Instructor
Faisal Rehman – Lead Instructor
Latesha Brown – Office Administrator

IT ProBasic Program

Learning Methodology: Resident, Hybrid IDL or Full IDL
Academic QCHs: 22.5
Clock Hours: 360
Enrollment Term: 15 or 21 weeks
Award Attainment: Certificate

Program Cost	$	10,549.50
Tuition	$	9,135.50
Curriculum[1]	$	1,314.00
Registration Fee[1]	$	100.00

[1] These items are non-refundable once the student starts and issued to the student

The ITPB Program consists of three courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance and networking. The coursework and practice tests prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals and Microsoft Azure AI Fundamentals. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The objective of this program is to provide the technical skills and knowledge identified in the course descriptions below along with the professional soft skills needed to start and maintain a career in the IT Industry. Job opportunities exist within all levels of the economy from government employment, employment with Fortune 100 and 500 companies, and small businesses. Opportunities exist in all types of settings for these types of positions such as:

- Level I, II and III Help Desk Support
- PC Repair Technicians
- Technical Support Engineers
- Technical Consultants

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Information Technology Security and Administration (ITSA)

Learning Methodology: Hybrid IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives
The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- Systems Administrators
- PC Repair Technicians
- Level I, II and III Help Desk Support
- Technical consultants

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent

Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident and Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Curriculum[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Curriculum[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:

ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network

infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States’ political history and improve students’ understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the

United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 — Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours — Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner

Tuition: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to recognize threats and manage risks in hardening an organization's security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course

Tuition: $495 | Enrollment Term: 12 weeks
Course Clock Hours: 18 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 24 weeks
Course Clock Hours: 18 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course

Tuition: $595
Enrollment Term: 30 weeks
Course Clock Hours: 36 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:

A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Indianapolis Programs and Campus Staff

2601 Fortune Circle East Suite 100c Indianapolis, IN 46241 ~ 317-550-3044

Campus Faculty & Staff

Diondraie Robertson – Asst. Dir. of Admissions (Site Coordinator)
Russ Munisteri – Program Chair
Kay Fogle – VA Specialist
Asia Jackson – Career Services Specialist
Carlos Garcia – Career Services Specialist
Enrica Kieselhorst – Career Services Specialist
Elizabeth Finley – Career Services Specialist
Jason Moreno – Career Services Specialist
Jewel McKnight – Career Services Specialist
Naina Hingher – Career Services Specialist
Paula Rendon – Career Services Specialist
Samantha Leon – Career Services Specialist
Shayla Kilpatrick – Career Services Specialist
Shweta Save – Career Services Specialist
Theresa Borden – Career Services Specialist
Jacob Bennett – Career Services Specialist
Kelsey Sandford – Career Services Specialist
Yusheka Garner – Admissions Advisor
Grace Terry – Admissions Advisor
Scott Henry – Admission Advisor
Rahmon Mallard – Admission Advisor
Jennifer Douty – Office Administrator
Nakia Moore – Career Advisor
Anthony Queen – Lead Instructor
Darryon Rivera – Lead Instructor
Charles Carter – Lead Instructor
Ray Downing – Lead Instructor
Terry Deckard – Lead Instructor
John Early – Lead Instructor
Mike Kalka – Lead Instructor
Kristin Wong – Lead Instructor
Scott Stromberg – Lead Instructor
Benjamin Smith – Lead Instructor
Brett Boyer – Lead Instructor
Josh Renihan – Lead Instructor
George Dehaven – Lead Instructor
Grant Gibson – Lead Instructor
Dara Cox (FT)
Judith Anderson (adjunct)
Lisa Kochevar (adjunct)
Tamika Boone (adjunct)
Tammy Bird (adjunct

Information Technology Security and Administration (ITSA)

Learning Methodology:	Resident, Hybrid IDL, Full IDL
Academic QCHs:	45,
Clock Hours:	720
Enrollment Term:	30 or 42 Weeks
Award Attainment:	Certificate

Program Cost	$21,097.00
Tuition	$18,271.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives

The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- Systems Administrators
- PC Repair Technicians
- Level I, II and III Help Desk Support
- Technical consultants

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,613.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and

Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition	$22,048.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student's skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of

vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program

is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the “bring your own device” (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident and Full IDL
QCHs: 112.5
Program Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087.00	Term One Curriculum[1]	$2,726
Tuition term one	$9,135.50	Term Three CEH Curriculum[1]	$1,072
Tuition term two	$9,135.50	Term Four Curriculum[1]	$2,435
Tuition term three	$11,024	Term Four CFR Curriculum[1]	$650
Tuition term four	$11,024	Term Five Gen Ed. Software[1]	$300
Tuition term five	$2,485	Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:

ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is

for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States’ political history and improve students’ understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic

business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials

Tuition and Fees: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker

Tuition and Fees: $3,640 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to recognize threats and manage risks in hardening an organization's security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course
Tuition: $495 Enrollment Term: 12 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course
Tuition: $595 Enrollment Term: 24 weeks
Course Clock Hours: 18 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course
Tuition: $595 Enrollment Term: 30 weeks
Course Clock Hours: 36 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

Bootcamps:
A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495
CompTIA CySA+ Test Prep Package
Tuition: $495
CompTIA CASP+ Test Prep Package
Tuition: $645
CISCO CCNA Test Prep Package
Tuition: $495
A+ Essentials 1 Certification Test Prep Package
Tuition: $495
CISCO CyberOps Certification Test Prep Package
Tuition: $495
CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645
Network+ Essentials Certification Test Prep Package
Tuition: $495
EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645
A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Columbus Programs and Campus Staff

4349 Easton Way Suite 145 Columbus, OH 43219 ~ 614-891-3200

Campus Faculty & Staff

Mike SanFilipo – Senior Director of Education (Site Coordinator)
Jeanne Ripper – Asst. Director of Admissions
Kay Fogle – VA Specialist
Tricia Mosher – Career Services Specialist, Lead
Alexandria Pierce – Career Services Specialist
Dakota Mahoney – Career Services Specialist
Harley Lacey – Career Services Specialist
Josie Anzaldua – Career Services Specialist
Joyce Sieben – Career Services Specialist
Margaret Peebles – Career Services Specialist
Martha Wallace – Career Services Specialist
Shareefah Dickens – Career Services Specialist
Fabian Pacheco – Career Services Specialist
Lynique McFadden – Career Services Specialist
Macey Luna – Career Services Specialist
Maricela Franco – Career Services Specialist
Sherman Williams – Career Services Specialist
Justin Jeffrey – Sr. Assistant Director of Admissions
Raeann Lee – Admission Advisor
Jamie Elzey– Admission Advisor
Brandon Hutcherson – Admission Advisor
Jeremy Townsend – Admission Advisor
Patrick McNeal – Admission Advisor
Leon Leavall – Admission Advisor
Shawn Kendrick – Admissions Advisor
John Skaggs – Admissions Advisor

Jerry Bastien – Lead Instructor
James Pariett – Lead Instructor
Alpesh Patel – Lead Instructor
Gearge Dehaven – Lead Instructor
Brett Boyer – Lead Instructor
Jason Queen – Lead Instructor
Wofgang Velasco – Lead Instructor
Grant Gibson – Lead Instructor
Josh Renihan – Lead Instructor
Dee Hudson – Lead Instructor
Ray Downing – Lead Instructor
Jill Schaumloeffel – Lead Instructor
Russ Munisteri – Lead Instructor
Jim Atria – Lead Instructor
Jeff Sims – Lead Instructor
Carlos Lewis – Lead Instructor
Michael Weekes – Lead Instructor
Lawrence Curtiss – Lead Instructor
Andrew Collins –Lead Instructor
Bo Bullington – Lead Instructor
Alex Kinyara – Lead Instructor
Servando Hernandez – Lead Instructor
Drew Collins – Lead Instructor
Candice Kiser – Lead Instructor
Emma Yake – Office Administrator
Lauren Connor – Live Online Office Administrator
Miranda Dayvolt – Live Online Office Administrator

Columbus, OH Accrediting Body Completion & Placement Results

Program	2022 Completion Rate	2022 Placement Rate	2023 Completion Rate	2023 Placement Rate	2024 Completion Rate	2024 Placement Rate
ITSA 30 week Hybrid IDL	100.00%	66.67%	83.05%	50.00%	78.13%	80.95%
ITSA 42 week Hybrid IDL	50.00%	0.00%	n/a	n/a	n/a	n/a
ITSA 30 week Full IDL	77.29%	52.36%	73.01%	52.39%	73.05%	73.25%
ITSA 42 week Full IDL	80.29%	57.58%	n/a	n/a	n/a	n/a
CSS 42 week Full IDL	90.83%	71.13%	92.54%	75.00%	n/a	n/a
CSS 30 week Full IDL	n/a	n/a	83.43%	70.08%	80.00%	80.43%
CSE 30 week Full IDL	n/a	n/a	95.29%	72.46%	91.25%	70.49%
CSE 42 week Full IDL	97.08%	70.75%	85.71%	78.79%	n/a	n/a
Associates Degree NACS Full IDL	80.00%	75.81%	87.02%	81.72%	76.92%	83.33%
Cyber Warrior Program Full IDL	n/a	n/a	91.79%	63.40%	93.47%	71.32%

n/a = program did not have any graduates.

Placement rate for prior year graduates as of May 1st. Placements after May 1st are not included in the rate.

Accreditation (ACCET) Placement Definitions

Information Technology Security and Administration (ITSA)

Learning Methodology: Resident, Hybrid IDL, or Full IDL
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$21,097.00
Tuition 1st Half	$9,135.50
Tuition 2nd Half	$9,135.50
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student	
[1] Refunds will be made in accordance with OAC 3332-1-10.1	

The IT Security and Administration program includes six courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, Microsoft Azure Fundamentals, Microsoft Azure AI Fundamentals, Linux Essentials, CompTIA Networking+, and CompTIA Security +. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives
The IT Security and Administration program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations.

- Technical support engineers
- Systems Administrators
- PC Repair Technicians
- Level I, II and III Help Desk Support
- Technical consultants

The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Computer and Security Essentials	30	90	120	1.5	6	7.5
Networking I	30	90	120	1.5	6	7.5
Operating Systems I	30	90	120	1.5	6	7.5
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5

Computer and Security Essentials: Students will be instructed on how to install and configure major computer and mobile device operating systems. Students will acquire the knowledge needed to secure device software, troubleshoot software issues encountered by computing devices, and understand the operational procedures involved with these devices in an enterprise network environment. Students are introduced to the communication and professionalism standards that exist in business operations.

Networking I: Students will be provided foundational information regarding computer hardware, associated components, and the techniques used to troubleshoot issues with these devices and components. Students will also be introduced to core networking concepts and troubleshooting, virtualization and cloud computing, and wireless technologies, and will engage in further exploration of mobile device concepts.

Operating Systems I: Students will be instructed on the fundamentals of both cloud computing and artificial intelligence. Students will gain an understanding of Microsoft Azure's core services, including cloud concepts, security, compliance, and pricing models, while also delving into the basics of artificial intelligence and machine learning. Students will be able

to make informed decisions on how to use the tools of AI technology for efficiencies and problem-solving within organizations.

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Cyber Security Specialist (CSS)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition 1st Half	$11,306.50
Tuition 2nd Half	$11,306.50
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,520.00
Registration Fee[1]	$100.00

[1] These items are non-refundable once the student starts and issued to the student.
[1] Refunds will be made in accordance with OAC 3332-1-10.1

The Cyber Security Specialist program includes six courses to prepare students to achieve System Administrator and Network Security Skills and knowledge. Completion of these courses will demonstrate skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system.

Vocational Objectives:
The Cyber Security Specialist program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organization. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to: Security Consultant, Systems Analyst, Firewall Engineer, Cisco Network Engineer, Infrastructure Network Engineer, Security Analyst, Data Security Engineer, IT Security Risk Management, Security Supervisor, Information System Security Specialist, Security Engineer, Information Security Officer, Threat & Vulnerability Analyst, Information Security Consultant, Protection & Control Specialist, and Windows Security. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: Linux Essentials, CompTIA Network+, CompTIA Security+, CCNA, CySA+, and Certified Ethical Hacker. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Server I	30	90	120	1.5	6	7.5
Security I	30	90	120	1.5	6	7.5
Networking and Security I	30	90	120	1.5	6	7.5
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5

Networking and Security VI	30	90	120	1.5	6	7.5

Server I: Students will be provided an overview of the Linux operating system and popular open-source applications. Students will understand the major components of Linux as well as security and administration-related topics and gain the knowledge to become technically proficient in working with Linux command lines, file management, and creating scripts.

Security I: The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Networking and Security I: Students will acquire the core knowledge required for cybersecurity roles including risk assessment and management, incident response, forensics, hybrid/cloud operations, and security controls. Emphasis is placed on the detection and remediation of security threats in an enterprise environment as well as the development of practical security troubleshooting skills.

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures.

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Cyber Security Engineer (CSE)

Learning Methodology: Full IDL
Prerequisites Required: See Enrollment Prerequisites on page 26
Academic QCHs: 45
Clock Hours: 720
Enrollment Term: 30 or 42 Weeks
Award Attainment: Certificate

Program Cost	$26,305.00
Tuition 1st Half	$11,024.00
Tuition 2nd Half	$11,024.00
CEH Curriculum[1]	$1,072.00
Curriculum[1]	$2,435.00
CFR Curriculum[1]	$650.00
Registration Fee[1]	$100.00
[1] These items are non-refundable once the student starts and issued to the student. [1] Refunds will be made in accordance with OAC 3332-1-10.1	

The Cyber Security Engineer program includes six courses to prepare students to achieve Network Security skills and knowledge. These courses demonstrate a student's skills in Network Infrastructure and Security. Upon completion of the program, the candidate will know how to plan, configure, and operate simple WAN and switched LAN networks. Students will also understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise

environment. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CCNA, CySA+, Certified Ethical Hacker, CCNA Security, CASP and the Cybersecurity First Responder. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost.

Vocational Objectives:
The Cyber Security Engineer program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The student will also have developed professional skills to assist in the obtainment of work and promotion in the IT industry. Examples of occupations include, but are not limited to:

- Cisco Network Engineers
- Information System Security Specialists
- Network Engineer
- Systems Administrators
- Threat & Vulnerability Analyst
- Security Analyst

Course Sequence and Descriptions:
Each course is typically 5-7 weeks at 17-24 hours per week. Courses can be taken in any order.

Course	Lecture	Lab	Total	Lecture	Lab	Acad QCHs
Networking and Security III	30	90	120	1.5	6	7.5
Networking and Security IV	30	90	120	1.5	6	7.5
Networking and Security VI	30	90	120	1.5	6	7.5
Networking and Security VIII	30	90	120	1.5	6	7.5
Networking and Security IX	30	90	120	1.5	6	7.5
Networking and Security X	30	90	120	1.5	6	7.5

Networking and Security III: Students will expand their IT knowledge by learning focused switch and router configuration strategies. These strategies include the exploration of network segmentation and routing protocols. Students will also learn how network devices communicate with each other to complete the flow of data. An expanded discussion of IP addresses will allow students to comprehend how networks are created and deployed. Techniques used to secure network equipment will also be examined throughout the course.

Networking and Security IV: Students will be introduced to the concepts of penetration testing. Students will be led through the practices used to gather information about network devices and the potential weaknesses that are present. An examination of the tools used by hackers and methods used to protect an infrastructure against them will be delivered. Students will be trained to recognize the governmental regulations that ensure company compliance and the industry frameworks used to design secure infrastructures

Networking and Security VI: Students will be trained to specifically identify, classify, and remediate threats to an organization, using threat research techniques. Students will be exposed to the practice of reading the output of vulnerability assessment tools and how to identify threats to specific types of technology. Emphasis will be placed on the procedural requirements of responding to an incident. Students will be presented with the procedures required to conduct an effective digital forensic investigation.

Networking and Security VIII: Students will learn the technical knowledge required to conceptualize, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise. This knowledge will include secure access implementations, virtualization and cloud solutions, and threat management activities. Students will also be trained in the use of industry tools used to identify infrastructure vulnerabilities and the strategies to reduce them. Students will be able to recognize forensic tools and their functions.

Networking and Security IX: Students will be given the opportunity to acquire the skills necessary to work in a Security Operations Center (SOC). The content presented addresses the ideas of defense-in-depth, attack vectors, attack surfaces, and data types. Students will also explore host-based security monitoring, malware analysis tools, and intrusion detection and prevention mechanisms.

Networking and Security X: Students will discuss the processes necessary to identify key areas of an organization's security posture, policies, and response methodology. Discussions related to hardware and software updates and patch management will enforce the importance of using defense-in-depth to protect assets. Students will learn to analyze log files and identify the appropriate responses to potential and actual breaches found within a network. The topics of Business Continuity and Disaster Recovery are explored to address the issue of business operations being maintained in the event of a breach.

Cyber Warrior Program (CWP)

Learning Methodology: Resident, Hybrid IDL, Full IDL
Academic QCH: 30
Clock Hours: 480
Enrollment Term: 12, 19, or 24 Weeks
Award Attainment: Certificate

12 Week Daytime CWP:

Program Cost	$23,805.00
Tuition	$20,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1]These items are non-refundable once the student starts and issued to the student	

19 or 24 Week Evening CWP:

Program Cost	$24,805.00
Tuition	$21,479.00
Curriculum[1]	$2,726.00
Registration Fee[1]	$100.00
Computer[1]	$500.00
[1] These items are non-refundable once the student starts and issued to the student	

The Cyber Warrior program includes five courses that provide the knowledge and skills to help students obtain a well-rounded IT education. Upon completion of the program, the candidate will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, web authentication, and extensive TCP/IP familiarity. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment. The coursework and practice tests within the program prepare students to sit for the following Industry exams: CompTIA A+, CompTIA N+, CompTIA Security+ and CySA+. All eligible students may receive at least one certification exam voucher upon request for each exam at no cost - Reference the Section: Certification Conditions.

Vocational Objectives:
The Cyber Warrior Program is designed for individuals seeking a career as an information technology (IT) professional working in the typically complex computing environment of medium to large organizations. The objective of this program is to provide the technical skills and knowledge identified below along with the professional soft skills needed to start and maintain a career in the IT Industry.

- Technical support engineers
- Technical consultants
- Security Analyst
- Threat & Vulnerability Analyst
- PC Repair Technicians
- Level I, II and III Help Desk Support

Course Sequence and Descriptions:
Each course is typically 2-3 weeks long at approximately 40 hours per week.

Course	Lecture	Lab	Total	Acad QCHs
Networking Concepts	20	60	80	5
Computer and Security Concepts	20	60	80	5
Security I	30	90	120	7.5
Security II	20	60	80	5
Security III	30	90	120	7.5
Totals	120	160	480	30

Networking Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with technical competency in networking administration and support. Students will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools, and network security.

Computer and Security Concepts (5 Academic QCHs, 80 Total Clock Hours): The purpose of this course is to provide students with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer components, laptops and portable devices, operating systems, printers and scanners, and networks. Students will be exposed to security concerns, safety and environmental issues, and fundamental troubleshooting skills in the areas of: Personal computers (PCs), Operating systems (OSs), Laptop/portable computers, Printers and scanners. Upon completion of this course, students will also be able to identify and explain the various concepts: Wired/wireless networks, Computer and network security, Proper employee communication and professionalism for business operations

Security I (7.5 Academic QCHs, 120 Total Clock Hours): The purpose of this course is to provide students with the requisite knowledge to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing Internet connectivity are covered. This course also focuses on securing business networks in the "bring your own device" (BYOD) environment that exists today.

Security II (5 Academic QCHs, 80 Total Clock Hours): In this course, students will learn how to secure and manage all facets of a network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

Security III (7.5 Academic QCHs, 120 Total Clock Hours): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

Associate of Applied Science in Network Administration and Cyber Security

Learning Methodology: Resident and Full IDL
QCHs: 112.5
Clock Hours: 1665
Enrollment Term: 85 - 119 Weeks
Award Attainment: Associate of Applied Science
Prerequisite: HS Diploma or equivalent

Program Cost	$50,087
Tuition term one	$9,135.50
Tuition term two	$9,135.50
Tuition term three	$11,024
Tuition term four	$11,024
Tuition term five	$2,485

Term One Curriculum[1]	$2,726
Term Three CEH Cur.[1]	$1,072
Term Four Curriculum[1]	$2,435
Term Four CFR Cur.[1]	$650
Term Five Gen Ed. Software[1]	$300
Registration Fee[1]	$100

[1] These items are non-refundable once the student starts and issued to the student. In accordance with OAC 3332-1-10.1

The Network Administration and Cyber Security program includes 12 core IT courses and five general education courses to obtain a well-rounded education. Upon completion of the first six courses, students will have valuable understanding and skills in basic hardware installation, troubleshooting and maintenance, networking and topology support, security configuration and analysis, as well as the configuration, securing, maintenance and troubleshooting of a computer network. This includes security measures, web authentication, and extensive TCP/IP familiarity. Upon completion of the next six IT courses, students will understand how to plan, configure, and operate simple WAN and switched LAN networks as well as know how intruders escalate privileges and what steps can be taken to secure a system. In addition, students will understand VLSM, IPv6, OSPF, and EIGRP protocols and learn to use access lists using NAT and DHCP. Students will be able to make the design and technology decisions necessary to ensure successful technology implementation projects. This includes Active Directory, security measures, web authentication, and extensive TCP/IP familiarity. The coursework and practice tests within the program prepare students to sit for the following Industry Certification exams: CompTIA A+, MTA Security Fundamentals, Linux Essentials, MTA Server Fundamentals, CompTIA Server+, MTA Server Fundamentals, CompTIA Server+, MTA Networking, CompTIA Network+, CompTIA Security+, CCNA, CySA+, Certified Ethical Hacker, CCNA Cyber ops, CASP and the Cybersecurity First Responder. All eligible students may receive at least 1 certification exam voucher upon request for each exam at no cost.

Course Descriptions:
ITPC 101 - Intro to PCs (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to identify, install, configure, upgrade and troubleshoot personal computer

components, laptops and portable devices, operating systems, printers and scanners, networks, security, understand safety and environmental issues, upgrade and troubleshoot personal computer components, operating systems, laptop/portable computers, printers and scanners. As well as, identify the fundamental principles of wired/wireless networks, computer security, safety, environmental issues, and proper employee communication and professionalism for business operations.

NET 101 - Intro to Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with technical competency in networking administration and support. The student will demonstrate critical knowledge of network technologies, media and topologies, network devices, network management, network tools and network security.

ITOS 101 - Operating Systems (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): This course introduces students to various types of operating systems. Emphasis is placed on overall concepts, installation, maintenance, management, resources, and security. Students will be introduced to operating systems from both a client and a server perspective.

SER 101 - Intro to Server (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): To provide the student with the knowledge necessary to implement, administer and troubleshoot a server environment.

CLI 201 – Security I (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hours): Students will learn how to secure and manage all facets of your network from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within your company's network infrastructure. This includes learning the knowledge of systems security, network infrastructure, access control, assessments, and audits.

NSEC 101 - Intro to Security and Networking (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hours, 6 QCH/90 Lab Hrs.): To provide the student with the knowledge necessary to plan, configure, and operate simple WAN and switched LAN networks. Topics such as IPv6 basics, network device security, and establishing internet connectivity are covered. This course also focuses on securing business networks in the BYOD environment that exists today.

NSEC 203 - Networking and Security III (7.5 QCH, 120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to configure, manage, and maintain routers in a complex networking environment. Students will learn to recognize evaluate the following terms: VLSM, OSPF, and EIGRP protocols in relation to network configuration and how to use Access Control Lists and NAT to secure a network environment. The primary objective for this course is for students to gain an understanding of what it takes to install and maintain routing devices in an Enterprise environment.

NSEC 204 - Networking and Security IV (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course will provide the knowledge and practical experience with the current essential security systems. Students will learn how intruders escalate privileges and what steps can be taken to secure a system. This course also focuses on addressing security issues to the latest operating systems and addresses developments in mobile and web technologies.

NSEC 206 - Networking and Security VI (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to identify malware and gain an understanding of the approach required to mitigate these threats. Students will also learn about Advanced Persistent Threats (APTs) allowing for them to gain an enhanced ability to recognize threats across a broad attack surface. Students will learn to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization.

NSEC 208 - Networking and Security VIII (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will gain the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise. Students will learn how to summarize business and industry influences and identify the security risks associated with those relationships. Students will also learn how to apply security mitigation strategies and controls in an Enterprise environment.

NSEC 209 - Networking and Security IX (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): This course is designed to prepare students to begin an IT career working alongside associate-level cybersecurity analysts in a security operations center. The content presented in this course will prepare students to take the “Understanding Cisco Cybersecurity Fundamentals” and “Implementing Cisco Cybersecurity Operations” certification exams. Instruction for the first portion of this course will focus on network concepts, security concepts, cryptography, host-based analysis, security monitoring, and attack methods. Instruction for the implementation portion of the course will focus on the topics of endpoint threat analysis and computer forensics, network intrusion analysis, incident response, data and event analysis, and incident handling.

NSEC 210 - Networking and Security X (7.5 QCH/120 Clock Hours: 1.5 QCH/30 Lecture Hrs. 6 QCH/90 Lab Hrs.): Students will learn how to apply security governance principles in alignment with business goals and organizational processes in an Enterprise environment. The legal and regulatory concerns related to information technology security enforcement will be reviewed in this course. Physical and virtual asset security is defined along with the concepts relative to applying security engineering in the business environment.

ENG 101 - English Composition I (4.5 QCH, 45 Clock Hours lecture): This course provides students the opportunity for extensive practice in critical reading and thinking as well as academic essay writing. Emphasis will be placed on the writing process and the organization and development of ideas. Students will develop their writing skills for the purpose of supporting a thesis statement. Students should also be able to respond critically to readings and demonstrate an understanding of the fundamentals of research and APA documentation.

COM 101 - Introduction to Communication (4.5 QCH, 45 Clock Hours lecture): This course introduces students to human communication. The theories and models that will be explored were selected to examine communication through a variety of contexts including interpersonal and group relationships, discussions on intercultural and gender contexts and concluding with public communication to an audience. Students will identify and differentiate aspects of human communication in academic, professional, and social settings as they engage in the course material. This course allows students to gain the knowledge needed to skillfully present a speech in a pro. setting.

GOV 101 - American Government (4.5 QCH, 45 Clock Hours lecture): This course will introduce students to the United States' political history and improve students' understanding of political institutions, elections, rights, freedoms, and policy issues. The critical lens provided in this class will take students through the founding and development of the United States; students will debate the structure of the United States republican form of government, connect the branches of government to contemporary politics and elections, and critique the American constitutional system. The overarching goal is for students to arrive at a deeper and more comprehensive understanding of the players that shape American government and politics so that students may become better informed and knowledgeable participants in American society.

PHI 101 - Philosophy (4.5 QCH, 45 Clock Hours lecture): This course is a critical introduction to the field of philosophical inquiry. After defining philosophy and identifying the major fields of philosophical study, the course examines the history of Western thought, from the famous Greek philosophers up to the cutting-edge intellectuals of today.

MAT 102 - Business Math (4.5 QCH, 45 Clock Hours lecture): This course is designed to provide students with a basic approach to business mathematics using a practical, skill-building approach. This course will provide students with basic business vocabulary and an understanding of financial statements, insurance, and investments. Students will conclude this course by creating amortization tables and constructing business charts based on statistical information.

Elective: **PSY 101 - Introduction to Psychology** (4.5 QCH, 45 Clock Hours lecture): This course is a survey of selected topics in psychology, including research methods, physiological psychology, sensation, perception, consciousness, learning, memory, motivation, gender roles, abnormal behavior, psychotherapy, and social psychology.

Seminars ~ IT Skill Sets - Avocational Offerings

Avocational Professional Development courses offered on the Raleigh, NC campus are designed for individuals that want to increase their knowledge and skill for Personal or Professional Development as well as individuals employed in the field that want to meet the requirements of their profession by completing a Continuing Education Course. Career Services and Job Placement assistance are not available for Avocational courses. See avocational online store for more information – https://upskillacademy.mycomputercareer.edu/.

A+ IT Essentials 1

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the foundational information regarding computer hardware, components, and the fundamental techniques used to troubleshoot issues. Students will also be introduced to managing core networking components, concepts, troubleshooting and identifying hardware solutions, virtualization, cloud computing, and wireless and mobile technologies.

A+ IT Essentials 2

Tuition and Fees: $3,490
Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours
Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will expand their knowledge to secure and troubleshoot device software issues. Operational procedures and troubleshooting for devices and enterprise networks will be a main focus. Students will also be introduced to professionalism and proper communications in a business environment.

Network+ IT Essentials
Tuition and Fees: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to manage, install, configure, and troubleshoot a computer network in a highly marketable and in-demand skill. This explores the fundamental building blocks that form a modern network, such as hardware, topologies, and protocols, along with an introduction to various network models. Provides in-depth coverage of the vital concepts in contemporary networking, including TCP/IP, Ethernet, wireless transmission, virtual networks, cloud computing, segmentation, security, performance optimization, troubleshooting, and network support.

Linux Essentials
Tuition and Fees: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will acquire knowledge and an overview of the Linux operating system. It explores the principles of open-source philosophy, licensing, and software and their relation to the Linux operating system. Students will examine various Linux distributions and software and storage management. The fundamentals of the BASH shell and security administration and user management best practices are covered, along with an understanding of system processes, package management, repositories, and cloud services.

CyberSecurity Specialist
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to secure and manage all facets of a network, from CPU cycles to software used by individuals or across a network. Students will learn how to implement and maintain an effective security strategy within a company's network infrastructure. This course will prepare students to sit for the CompTIA Security+ certification exam or similar.

CyberSecurity Ethical Hacker
Tuition and Fees: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills of computer security and penetration testing. It will provide students with skills to protect institutions and businesses, administer security testing procedures, recognize the legal ramifications of penetration testing and reduce the security vulnerabilities that businesses and institutions face today. This course will prepare students to sit for the EC-Council Certified Ethical Hacking (CEH) certification exam or similar.

CyberSecurity First Responder
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn a comprehensive approach to develop the skills to monitor and detect security incidents in information systems and networks, execute a proper response to such incidents, identify various types of common threats, evaluate an organization’s security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This course will prepare students to sit for the CertNexus CyberSecurity First Responder (CFR) cert exam or similar.

CyberSecurity Advanced Practitioner
Tuition: $3,640 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn the skills to recognize threats and manage risks in hardening an organization’s security posture. Risk management frameworks will be explored to assess and mitigate risk, identify threat actors and physical risks, reduce risks related to human resources and social engineering techniques, examine qualitative and quantitative risk analysis, and identify insider threats, supply chain dependencies, and sources of threat intelligence. This course will prepare students to sit for the CompTIA CASP+ certification exam or similar.

Cisco Networking Essentials
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL
In this course, students will learn theory and demonstrate skills to understand network fundamentals, network access, IP connectivity and services, and network security fundamentals, laying the foundation for network automation and programmability. This course will prepare students to sit for the Cisco CCNA certification exam or similar.

CyberSecurity Analyst
Tuition: $3,490 Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses. This course will prepare students to sit for the CompTIA CySA+ certification exam or similar.

Cisco Cyber Operations Specialist

Tuition: $3,490 | Enrollment Term: 1-5 weeks
Course Clock Hours: 40 or 60 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

In this course, students will learn the skills related to security concepts and monitoring of host-based analysis, network intrusion analysis, security policies and procedures, common network and application operations, attacks, and the types of data to investigate security incidents. In addition, it provides the understanding to monitor alerts and breaches to understand procedures for various incidents. This course will prepare students to sit for the Cisco CyberOps certification exam or similar.

Cyber 12-Week Certification Mastery Course

Tuition: $495 | Enrollment Term: 12 weeks
Course Clock Hours: 18 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Cyber 24-Week Certification Mastery Course

Tuition: $595 | Enrollment Term: 24 weeks
Course Clock Hours: 18 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following CompTIA certification exams: A+, Network+, Security+ and CySA+.

Security Administration 30-Week Certification Mastery Course

Tuition: $595 | Enrollment Term: 30 weeks
Course Clock Hours: 36 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

This course will provide students with the opportunity to gain additional instruction to aid in passing the following certification exams: A+, Network+, LPI Linux Essentials, Microsoft Azure Fundamentals, Microsoft AI Fundamentals, and Security+

The MyComputerCareer Ultimate Salesforce Fundamentals Course

Tuition: $2,100 | Enrollment Term: 4 weeks
Course Clock Hours: 48 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

The MyComputerCareer Ultimate Salesforce Fundamentals Course includes Microsoft Excel Basics, Microsoft Excel Formulas, Salesforce Classic for End Users and Salesforce Lightning for End Users to help students obtain foundational knowledge and skills to use the Salesforce platform effectively. Upon completion of the course, the candidate will have a working knowledge of Microsoft Excel including its features, functions, and formulas as well as insight into the functionality of Salesforce Classic and Salesforce Lightning including how to create contacts, leads, opportunities, accounts, and cases and applying Chatter and Campaign functions to communicate.

The MyComputerCareer Ultimate Salesforce Administrator Course

Tuition: $5,650 | Enrollment Term: 8 weeks
Course Clock Hours: 96 hours | Learning Methodology: Resident, Hybrid IDL, Full IDL

The MyComputerCareer Ultimate Salesforce Administrator Course focuses on administrative features and functionality of Salesforce to implement, configure, and manage Salesforce applications with an introduction to Apex Programming Language. Upon completion of the course, the candidate will have a practical knowledge of basic administrator functions including organization and user set up, security and access, sales and marketing applications, activity management and collaboration, standard and custom objects, workflow/process automation, data management and analytics. The coursework and practice tests within the course prepare students to sit for the Salesforce Administrator Certification Exam. All eligible students may receive at least one certification exam voucher upon request for the exam at no cost.

Ultimate Salesforce Fundamentals and Administrator Course Bundle

The cost of both courses when they are purchased together at the time of enrollment: Tuition and Fees: $5,950

Bootcamps:
A one day, four-hour comprehensive review of test prep questions with a live instructor, along with student engagement, on pertinent topics that will help prepare students for the respective industry certification exams:

CompTIA Security+ Test Prep Package
Tuition: $495

CompTIA CySA+ Test Prep Package
Tuition: $495

CompTIA CASP+ Test Prep Package
Tuition: $645

CISCO CCNA Test Prep Package
Tuition: $495

A+ Essentials 1 Certification Test Prep Package
Tuition: $495

CISCO CyberOps Certification Test Prep Package
Tuition: $495

CyberSec Certified First Responder Certification Test Prep Package
Tuition: $645

Network+ Essentials Certification Test Prep Package
Tuition: $495

EC Council Certified Ethical Hacker Test Prep Package
Tuition: $645

A+ Essentials 2 Certification Test Prep Package
Tuition: $495

Apex Non-Instructional Branch

Apex, North Carolina (919) 278-7922

Please note this Apex branch does not provide instruction to students and does not have educational facilities for student access.

Director of Contact Center: Deborah Grygoruk

Assistant Directors of the Contact Center: Emily Price, Nakia Moor, Crystal Avery

Trainer/Team Lead: Maggie Doyle

Team Lead: Hailey Phillips

Success Coordinators:

Michael Woods
Laura Volkmar
Ruby Ayers
Dhiren Patel
Jaren Hill
Anolani Kane
Mike Rumble
Stacy Wharton
Imani Smith
Tiffani Dixon
Brooklyn Washburn
Madison Schmitz
Hayden Haggarrd
Skylar Vitale
Jazmin Parker
Anika HIckman
Kayla Garcia
Amber Glasper
Lisa Ford
Isaac Kinity
Michael Green
Nkiruka Chimebele
Kristen Chaney
Kymari Miller
Larmeisha Neal
Stacy Driver
Rebekah Ukoh
Andrew Sabio
Milan White

LOCATIONS:

Raleigh, NC
Charlotte, NC
Indianapolis, IN
Sugar Land, TX
Houston, TX
Dallas, TX
Arlington, TX
Columbus, OH
Nellis Air Force Base, NV
Live Online

MYCOMPUTER CAREER

TRAINING FOR A BETTER LIFE

mycomputercareer.edu | (866) 606-6922