Cybersecurity Institute at Lab Four

Student Handbook and Catalog

February 19, 2026
2026-2027

Expires June 30, 2027

Welcome to your future.

Cybersecurity Institute at Lab Four

1255 Lynnfield Road, Suite 160
Memphis, TN 38119

901-261-1111

www.labfour.com

Accredited by ACCET – A Partnership for Quality®

Cybersecurity Institute at Lab Four is authorized by the Tennessee Higher Education Commission. This authorization is based on an evaluation of minimum standards concerning the provision of education, ethical business practices, and fiscal responsibility.

State of Tennessee
Tennessee Higher Education Commission
312 Rosa Parks Ave, 9th Floor
Nashville, TN 37243
(615) 741-3605

TABLE OF CONTENTS

MISSION STATEMENT

Cybersecurity Institute at Lab Four's mission is to become a key workforce development partner in three ways: by providing the best possible technology training to help businesses become more successful; providing the skills and credentials necessary for individuals to secure stable employment or pursue entrepreneurship opportunities in a high-demand industry; and partnering with nonprofit organizations to help our community fulfill its vast potential. We will accomplish this through the most innovative, effective, and ethical methods possible from top to bottom.

HISTORY OF LAB FOUR

Cybersecurity Institute at Lab Four began in 2008 as an outgrowth of an Information Technology (IT) company called Lan One (now Lab Four Systems) whose history dates to 1998. We formed in response to workforce development needs identified in our local community of Memphis, TN. Acknowledging both the widening technology skills gap employers face and the reality that individuals stuck in low-paying, low-skilled jobs are highly unlikely ever to escape the cycle of poverty without increased access to training and tangible opportunities for career advancement, we set out to create and provide those opportunities and connections. The transition from *getting by* to *getting ahead* requires several steps; one of which is technical training in preparation to obtain industry certifications in a high-demand field. Lab Four also provides coaching through the steps of entering and navigating a sustainable career in tech, with real growth potential.

PERFORMANCE

We measure success not by our enrollment numbers or even by how many people complete training programs each year; but by our training-related employment and entrepreneurship placement rate. Below is a snapshot of our completion and placement outcomes for vocational programs over the past five years:

Performance for 2020-2024	
Program Completion Rate:	90.28%
Training-Related Job Placement Rate:	73.15%

ACCREDITATION

Cybersecurity Institute at Lab Four is accredited by the Accrediting Council for Continuing Education and Training (ACCET), and recognized by the US Department of Education (ED) in The Database of Accredited Postsecondary Institutions and Programs (follow this link: http://ope.ed.gov/accreditation/Search.aspx and search "Lab Four").

AUTHORIZATION STATEMENT

Cybersecurity Institute at Lab Four is authorized by the Tennessee Higher Education Commission. This authorization is based on an evaluation of minimum standards concerning the provision of education, ethical business practices, and fiscal responsibility.

State of Tennessee
Tennessee Higher Education Commission
312 Rosa Parks Ave, 9th Floor
Nashville, TN 37243
(615) 741-3605

GOVERNING BOARD OF DIRECTORS

Cybersecurity Institute at Lab Four is a Tennessee Non-Profit Corporation. Its Board of Directors includes:

- Stephanie Okhiria (Executive Director, Treasurer)
- Tony Okhiria (Board Member)
- Francis Oigbokie (Board Member)
- JC Scott (Board Member)

BRANCHES

Cybersecurity Institute at Lab Four, Memphis (Main) (901-261-1111) – 1255 Lynnfield Road, Suite 160, Memphis TN 38119

FACILITIES

Lab Four's classroom and administrative offices are located at 1255 Lynnfield Road, Ste. 160, Memphis, TN 38119. The facilities include five classrooms ranging in capacity from 10 to 25 students, advising and administrative offices, a break room, testing center, and conference rooms. The facility is handicap accessible and is also protected by 24-hour video and/or audio surveillance.

EDUCATIONAL EQUIPMENT

- Computers
- Overhead Projectors
- Desks
- Chairs
- Whiteboards
- Training Videos
- Network Cabling Tools
- Virtual Equipment
- Books/Manuals
- Conference Table
- Printers/Copiers
- Cabling workbench
- Audio Visual Stands
- DVDs/CDs
- Televisions
- Calculators
- Bookcases

ACADEMIC CALENDAR AND COURSE SCHEDULE

Cybersecurity Institute at Lab Four is non-term oriented and has open enrollment. Course lengths vary according to each program, though the academic week typically consists of two 4.5 or 5-hour sessions on two separate days. Full-time enrollment status is considered to be 18 clock hours or more per week.

Courses are available in the following time slots for all programs, and begin according to demand (approx. once every 1-3 months):

9:30am-2:00pm M/W
9:30am-2:30pm M/W
1:00pm-5:30pm M/W
5:30pm-10:30pm M/W
6:00pm-10:30pm M/W

9:30am-2:00pm T/TH
9:30am-2:30pm T/TH
1:00pm-5:30pm T/TH
5:30pm-10:30pm T/TH
6:00pm-10:30pm T/TH

9:00am-4:00pm FRI
9:00am-4:00pm SAT

The following scheduling options are offered based on the total clock hours for each program. Please note, all scheduling options may not always be available at all times.

Clock Hours	Option 1	Option 2	Option 3
22.5	6 hours per week 4 weeks (final week = 4.5 hours) Class meets 2 days per week 9:00am – 12:00pm; 1:00pm – 4:00pm; or 6:00pm – 9:00pm	9 hours per week 3 weeks (final week = 4.5 hours) Class meets 2 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm	12 hours per week 2 weeks (final week = 10.5 hours) Class meets 3 days per week 9:00am – 1:00pm; 1:30pm – 5:30pm; or 6:00pm – 10:00pm
66	6 hours per week 11 weeks Class meets 2 days per week 9:00am – 12:00pm; 1:00pm – 4:00pm; or 6:00pm – 9:00pm	9 hours per week 8 weeks (final week = 3 hours) Class meets 2 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm	18 hours per week 4 weeks (final week = 12 hours) Class meets 4 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm
72	6 hours per week 12 weeks Class meets 2 days per week 9:00am – 12:00pm; 1:00pm – 4:00pm; or 6:00pm – 9:00pm	9 hours per week 8 weeks Class meets 2 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm	18 hours per week 4 weeks Class meets 4 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm
144	6 hours per week 24 weeks Class meets 2 days per week 9:00am – 12:00pm; 1:00pm – 4:00pm; or 6:00pm – 9:00pm	9 hours per week 16 weeks Class meets 2 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm	18 hours per week 8 weeks Class meets 4 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm
301	9 hours per week 34 weeks (final week = 4 hours) Class meets 2 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm	12 hours per week 26 weeks (final week = 1 hour) Class meets 3 days per week 9:00am – 1:00pm; 1:30pm – 5:30pm; or 6:00pm – 10:00pm	18 hours per week 17 weeks (final week = 13 hours) Class meets 4 days per week 9:30am – 2:00pm; or 6:00pm – 10:30pm
600	20 hours per week 30 weeks Class meets 4 days per week 9:30am – 2:30pm; or 5:30pm – 10:30pm	24 hours per week 25 weeks Class meets 4 days per week 9:00am – 3:00pm; or 4:30pm – 10:30pm	N/A

Hours of Operation

*Monday-Thursday: 8:00am – 10:30pm (**note**: if no evening class is in session on any Monday-Thursday, we will close at 5:00pm)*
Friday: 8:00am – 5:00pm
Saturday: 9:00am – 4:00pm
Closed Sunday

The school will be closed on the following 11 holidays:

1. *New Year's Day*
2. *Martin Luther King Jr. Day*
3. *Memorial Day*
4. *Juneteenth National Independence Day*
5. *Independence Day*
6. *Labor Day*
7. *Day Before Thanksgiving*
8. *Thanksgiving Day*
9. *Christmas Eve*
10. *Christmas Day*
11. *New Year's Eve*

Students will be notified of any other closing. In the event a start date falls on a listed holiday, class for that slot will begin the following week. Please contact your Career Specialist for questions regarding your schedule.

ADMISSION STANDARDS

Admission is open to all people aged 18 or older who have a high school diploma or equivalent. Each applicant must provide an official high school transcript, official GED score, or official military document indicating completion of high school; and complete all Application and Enrollment Documents prior to beginning any program. Academic, certification, and/or experience prerequisites do apply to some programs and are listed where applicable on the individual program description pages included in this catalog.

ENROLLMENT POLICIES AND GUIDELINES

A member of the Enrollment Team will ascertain prospective students' ability to enroll in a Cybersecurity Institute at Lab Four program during the admissions process. Prospective students are walked through the various program offerings and expected outcomes; the scholarship, grant, and financial aid options for which they may qualify; and the delivery mode options (i.e. on-site/residential, or online via interactive distance learning).

Once a funding option is selected and the applicant completes the Program Advising process to determine which program(s) are best suited for them, the Enrollment Team member guides them through the application process toward admission, funding approval, and enrollment. Enrollment Team members provide a general overview of the program expectations, including Satisfactory Academic Progress (SAP) and Attendance requirements. They also discuss any required prerequisites for the program(s) in which the applicant is seeking to enroll; as well as any equipment or supplies required for the program that are not provided by Cybersecurity Institute at Lab Four and included with tuition and fees. Prior to admission, each applicant must complete the Application Packet electronically via the Student Portal (Verity), including an Interactive Distance Learning (IDL) Student Disclosure Form (Appendix 3 of this handbook) if they are opting for the IDL delivery mode.

Once approved, the applicant is admitted into the training program and converted into a Student to complete the educational requirements. Prior to the start of class, Students must complete the Enrollment document packet via the Student Portal (Verity), and participate in a New Student Orientation session.

Students are enrolled for the start of the next available session of their desired program(s). Students may only enroll in a program before the class begins or prior to the Add/Drop Deadline, which falls at one eighth of the total program length for programs consisting of only one class. For programs consisting of multiple classes, students must begin each individual class prior to its own Add/Drop Deadline. Program length is measured in contact (clock) hours. All students are subject to the same completion requirements, detailed in this handbook, including both attendance and Satisfactory Academic Progress, regardless of their enrollment date. Students joining a class late (between the class start and the Add/Drop Deadline) have the option of making up the clock hours missed by working directly with their instructor or by attending the corresponding class days of another cohort in the same program.

Any prospective student who has a special needs request or accommodation must submit the request in writing via email to the Campus Director prior to enrollment to determine if the school can accommodate the request.

Non-immigrant foreign students will be enrolled under the appropriate visa status, which is (a) M visa for vocational and/or technical programs, or (b) F visa for academic and language (avocational) programs, consistent with federal requirements.

All students enrolling in a class must have their tuition paid in full, or have secured funding approval from a grant, scholarship, or other funding source covering at least 40% of tuition before they can attend class. If there is a balance remaining after the initial payment or funding approval is applied, the student must either pay the remaining balance or finalize a payment plan prior to enrollment. If payment or funding approval is delayed beyond the Add/Drop Deadline, students will be placed on the roster for the next class of the same name and will be given a new start date upon receipt of payment or funding approval.

POLICY ON NON-DISCRIMINATION

Cybersecurity Institute at Lab Four does not discriminate nor condone discrimination on the basis of race, color, national origin, sex, gender, sexual orientation, religion, age, disability, or any other legally protected characteristic in employment or the provision of services.

TRANSFER OF CREDIT POLICY

Lab Four may accept credit earned at another institution only if that institution is accredited by an agency recognized by either the U.S. Department of Education or the Council for Higher Education Accreditation.

Accreditation is not, however, the sole factor in determining the acceptability of the credits for transfer from the institution at which they were earned. The following criteria must also be met for prior credit to be considered for transfer to Lab Four:

1. Minimum GPA of 1.0, "D" average, or "Pass" if the institution uses a Pass/Fail only grading system.
2. The student must provide, along with the Student Request for Transfer of Credit, the following items:
   a. An transcript from the institution from which credit is to be transferred
   b. A course description and/or syllabus of the applicable course(s) from the institution from which credit is to be transferred
3. The course description or syllabus provided with the Student Request for Transfer of Credit must be at least 25% comparable to that of the Lab Four program to which the student wishes to transfer credit and confirm that the course requirements conform to industry training standards in the subject area.

Degree Programs

Lab four uses quarter credit hours to define the length of its Occupational Associate Degree (OAD) programs. Students seeking transfer credit for any course within the OAD program that provides training toward an industry certification must provide proof that they have passed the industry certification exam or obtained equivalent competency through prior training and/or work experience. Those who do not hold the relevant industry certification must pass an equivalent course practice exam with a score of 70% or higher. General Education courses in the OAD program do not require an exam for transfer credit review but are subject to the requirements listed above. If approved for transfer of credit, students will receive the full quarter credit hours for the applicable approved course – no partial transfer of credit will occur for any individual course.

Upon approval of transfer of credit toward an OAD program, students will be charged a pro-rata portion of the standard tuition, based on the remaining courses they will be required to attend to complete the program after transfer credit is applied. Additional fees (such as for course materials distributed and attributable to the portion of the program attended by the student) are not affected by transfer of credit.

Certificate Programs

Lab Four uses contact (clock) hours to define the length of its vocational and avocational certificate programs. Classes are generally broken up into either 4.5 or 5-hour sessions meeting two to four days per week for the duration of the program. The number of hours transferrable to a Lab Four program, if approved, is limited and ranges from 16.67% to 83.33% of the total class hours rounded to the nearest whole class session, depending on the total length of the certificate program. If approved for transfer of credit, students will usually receive the full number of transferrable hours – no partial transfer of credit will occur except in the case of a 600-clock-hour program. For a 600-hour program, students may earn transfer credit for up to five of the six 100-hour courses within that program.

Upon approval of transfer of credit toward a certificate program, students will be charged a pro-rata portion of the standard tuition for the program in which they are to enroll, based on the number of hours they will be required to attend after the transfer of credit. Additional fees (such as for course materials distributed and attributable to the portion of the program attended by the student) are not affected by transfer of credit.

The table below illustrates the total hours transferrable for each possible "total contact hour" amount for all approved vocational and avocational certificate programs offered by Lab Four, as well as the tuition charged if/when transfer of credit is approved.

Total Contact Hours	Hours Transferrable (if approved)	Adjustment of Tuition
22.5	4.5	80.00% of standard tuition
66	13.5	79.55% of standard tuition
72	18	75.00% of standard tuition
144	36	75.00% of standard tuition
301	72	76.08% of standard tuition
600	100	83.33% of standard tuition
	200	66.67% of standard tuition
	300	50.00% of standard tuition
	400	33.33% of standard tuition
	500	16.67% of standard tuition

Lab Four is not currently eligible for federal financial aid. Once approved, however, ramifications for financial aid will mirror those established above for tuition without financial aid. Tuition will be adjusted to reflect a pro-rata portion for the total hours the student is required to attend after the transfer of credit. Additional fees (such as for course materials distributed and attributable to the portion of the program attended by the student) are not affected by transfer of credit.

There is no fee associated with the Student Request for Transfer of Credit.

Procedures to be followed when requesting transfer of credit:

1. During Program Advising, the Career Specialist will inform each prospective student that they have the option of requesting transfer of credit.
   a. The Program Advising form also includes a notice to prospective students with this information.
2. If the prospective student is interested in applying for transfer of credit, the Career Specialist advises the student to begin gathering the necessary documentation right away, and provides them with the Student Request for Transfer of Credit form, which requires the following:
   a. Transcript from the institution from which credit is to be transferred.
   b. Course description(s) and/or syllabi from the course(s) at the institution from which credit is to be transferred.
   c. The request is due ten calendar days prior to the student's projected program start date. If the student begins class without requesting transfer of credit in a timely manner or obtaining approval for transfer of credit, their application for transfer of credit will be considered void.
3. Submit the request via email to help@labfour.edu with the subject line "Request for Transfer of Credit – (Student Name)."
4. Once the Student Request for Transfer of Credit is submitted, the student will receive a decision from the Admissions Group (Enrollment Manager, Director of Compliance, and Academic Director) within three calendar days. The decision will come in the form of a letter (sent via email) containing either:
   a. Notification of acceptance of the student's request for transfer of credit. The acceptance letter will include the number of hours transferred, the new total hours the student is required to attend to complete the program, and the adjusted tuition resulting from the transfer of credit; or
   b. Notification of denial of the student's request for transfer of credit. The denial letter will include the reasoning behind the Admissions Group's decision, as well as the appeal process described below, should the student choose to appeal the decision.

Procedures to be followed when appealing a negative decision for transfer of credit:

1. Once notified of denial of the request for transfer of credit, the student has three calendar days from the date of the denial letter to submit an appeal to Senior Management if they choose. If the student begins class without requesting transfer of credit in a timely manner or obtaining approval for transfer of credit, their application for transfer of credit will be considered void.
2. The student's appeal is to include:
   a. A letter from the student describing why they disagree with the Admission Group's decision and presenting any new information or reasoning to be considered as part of the student's request.
   b. Any additional supporting documentation that the student can provide to support their claims.
3. Submit the appeal via email to help@labfour.edu with the subject line "Appeal for Transfer of Credit – (Student Name)."
4. Senior Management will deliver a final decision to the student in the form of a letter (sent via email) within three calendar days of when the appeal is submitted.

Transferability of credit from Lab Four to another institution:
If a student is attempting to transfer Lab Four credits to another institution, they may contact Admissions via help@labfour.edu to request any of the following:

1. Official Transcript
2. Program Description(s)
3. Syllabi or Course Outline(s)

Admissions will also give guidance as needed/requested on transferring credit earned at Lab Four, however the acceptance of credits earned at Lab Four is entirely dependent on the receiving institution's policies and practices. Lab Four does not guarantee the transfer of credits to any other institution. Students are advised to contact any educational institutions to which they may want to transfer credit earned at Lab Four to determine if such credit can be accepted for transfer prior to executing an enrollment agreement with Lab Four.

Transferability of credit between Lab Four locations:
Credit earned at any Lab Four location is eligible for transfer to any other Lab Four location, provided it meets the criteria described above (i.e. the student earned a passing grade, the course completed is at least 25% comparable to the course to which transfer credit is to be applied, etc.).

ATTENDANCE POLICY

Attendance and Class Participation are critical to the success of Students enrolled in Lab Four programs. Absences, tardiness, and early departures can prevent academic success and hinder progress toward career goals. Students must provide accurate *Time In* and *Time Out* for each class session, either by using the attendance app feature in the Student Portal **or** by signing a physical Class Attendance sheet. Students enrolled in Interactive Distance Learning (IDL) programs must also respond to Engagement Check questions posted in Microsoft Teams for Education for each hour of their scheduled class time, to verify their presence in the active class session. Attendance is monitored by the Instructor and managed by a designated Office Support Specialist on a weekly basis. This policy applies to all programs.

Additional guidelines for class attendance:

- **It is the Student's responsibility to ensure their attendance is properly recorded.** Attendance is documented electronically using the mobile app version of the Student Portal, accessed via each Student's own unique username and password. Students must *Check In* when they arrive for each class session and *Check Out* when they leave for the software to calculate their accurate time in attendance.
- Students are expected to attend each scheduled class session on time and participate actively in class. This includes both lecture and lab class sessions. **No absence excuses a Student from completing the required clock hours for their program.**
- To verify their presence and participation in the virtual classroom, Students enrolled in Interactive Distance Learning (IDL) courses must respond to an *Engagement Check* question posted each hour of the scheduled class session via Microsoft Forms in Microsoft Teams for Education. *This is in addition to IDL Students logging their time in and out of each class session via the Student Portal.*
    - Each *Engagement Check* question will be available for 15 minutes only (e.g. Question 1 is available from 7:00pm until 7:15pm; Question 2 is available from 8:00pm until 8:15pm; and so on)
    - *Engagement Check* questions are automated and cannot be retrieved once the scheduled window to answer is closed
    - Students who fail to respond to an *Engagement Check* question will not receive credit for attendance during that hour of class, regardless of whether they are *Checked In* during that time
- **Training on the technology associated with recording attendance is provided during the New Student Orientation, as well as on the first day of class. In the event of any technical issues, Students should reach out to support@labfour.edu. For any other questions related to recording or correcting attendance, contact sap@labfour.edu.**
- Students must attend *at least* **80%** of the clock hours scheduled for their program, including tardiness and early departures, to meet completion requirements. Students who fail to achieve **80%** attendance in their program will be subject to a Corrective Action Plan or forced withdrawal from the class. Absences may be consecutive or non-consecutive. Students must maintain this rate of participation to achieve Satisfactory Academic Progress. Therefore, absences must be kept to a minimum.
- A "clock hour" (or "contact hour") is defined as actual directed or supervised instructional time, not to be less than 50 minutes for every 60 minutes of time. A single clock hour also may not exceed 60 minutes.
- 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.
- **Any Student who is absent for 14 consecutive calendar days is subject to immediate withdrawal from the program.**
- **Any Student whose attendance rate is below the required 80% of clock hours expected to date at the midpoint of their program is subject to immediate withdrawal.**
- Lab Four does permit a Leave of Absence not to exceed 180 calendar days when a Student faces a temporary problem such as military deployment, accident, death in the family, or other emergency as long as there is a reasonable expectation the Student will return to the program prior to the expiration of the LOA.
- Make-up work must be similar to the class hours missed in content, time, and delivery. Make-up attendance must be documented accurately via the electronic Student Portal app or on a physical class attendance sheet.
- Students can only be given credit for attendance for the time the class is in session as verified by the Instructor. For example, a Student who records a Time In (or *Check In*) of 5:00pm and time out of 10:30pm for a class session held from 6:00pm until 10:30pm will only be credited for attending class from 6:00pm until 10:30pm. The Student would receive credit for 4.5 hours in attendance, not 5.5 hours.

Students whose attendance falls below **80%** of the hours offered at any point during the class will be contacted either by phone or email by their Instructor, their Career Specialist, or the designated Office Support Specialist (who holds primary responsibility for ensuring that this is done). This contact will be documented in the SAP Documentation Repository. In this communication, the Lab Four representative will inform the Student of their Attendance status (e.g. "You've missed a total of XX hours. You must attend XX hours total.")

ABSENCES

Students are expected to attend each class session on time and participate actively in each class session. 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 the scheduled clock hours for any program or course can be grounds for dismissal from the program.

Students with no attendance for 14 consecutive calendar days are subject to dismissal for violation of the Attendance Policy. Dismissed students must submit an appeal to the Campus Director within 10 days of termination. Approval of appeal is at the discretion of the Appeals Committee. Please reference the Appeal Process on page 14.

MAKE-UP WORK

Students that need to complete missed assignments and receive additional review of topics missed in class may do so. Make-up attendance must be documented accurately using the electronic Student Portal app, or by signing a physical make-up class attendance sheet. For students enrolled in Interactive Distance Learning (IDL) programs, make-up class sessions are held in the *Make-Up* class team inside Microsoft Teams for Education. The *Make-Up* class team contains multiple channels corresponding to all active Course IDs, matching the class team names where regular classes are held. Scheduled make-up sessions are found in the appropriate channel for the relevant class, ready to be joined at the start time.

Students who fail to complete and properly document sufficient make-up hours and assignments to regain compliance with attendance and cumulative grade requirements, or meet course completion criteria by the Academic Deadline, are subject to administrative withdrawal as outlined in the Satisfactory Academic Progress Policy.

TARDINESS AND EARLY DEPARTURES

Students are expected to be on time for all class sessions. 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 recording their “Time In” immediately upon arrival and their “Time Out” immediately upon departure. Consistent tardiness can adversely affect the learning environment and can be considered a violation of the Student Conduct Policy.

Regular or excessive tardiness or early departures can put a student at risk for dismissal from the training program due to not meeting the required hours of attendance (minimum 80%), per the Attendance and Satisfactory Academic Progress Policies. If the student does not meet 80% attendance at the midpoint of their program, the student is subject to immediate withdrawal. If the student appeals the withdrawal decision and the appeal is approved, the student will be placed on Academic Probation-and an academic plan will be provided to them. This plan must allow the student to meet SAP standards by the Maximum Time Frame of the program. Students on Academic Probation will continue to be evaluated at the regular scheduled intervals per the Satisfactory Academic Progress Policy.

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 Campus Director 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 Campus Director. 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 Lab Four. In order for a leave of absence to be granted, Lab Four must have a reasonable expectation that the student will return to the program at the end of the leave of absence. Students returning from a leave of absence will restart at the appropriate place during the next available class as determined by the Campus Director. If a student fails to reenter the class at the end of the leave of absence, the student will be academically terminated (withdrawn) from the program. Students have 10 days to appeal termination. Leaves of absence are 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.

REPEATS, INCOMPLETE AND REMEDIAL COURSES, COURSE WITHDRAWALS, AND TERMS

Repeat subjects in the classroom training environment are generally not allowed and any exceptions must be discussed with the instructor for the class and the Campus Director. Any assignments and/or clock hours completed during a course repeat will be added to the qualitative and quantitative measurements that will be evaluated at the next evaluation point. Because Lab Four is focused on overall competency by program completion, students can, during a repeat or at any other time prior to their maximum time frame, repeat graded work and if a higher score is achieved, the lower grade will be replaced.

Lab Four does not utilize an incomplete grade status, does not allow individual course withdrawals nor offer remedial programs. We do not offer summer terms, therefore all periods of enrollment count towards Satisfactory Academic Progress.

VISITORS

The Campus Director 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 is prohibited.

SOFTWARE PIRACY, COPYRIGHT LAWS, AND INTERNET USE

Lab Four strictly prohibits the piracy of software and the violation of piracy and copyright laws. Lab Four reserves the right to dismiss students from the program who are found to be using the equipment of Lab Four 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. 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.

Students may not share copyrighted materials, including syllabi, coursework, hand-outs, etc., with anyone else, including other students. Instructors are responsible for the appropriate dissemination of materials.

Students are also not allowed to pass down previous materials to new students, as materials are subject to change as the competencies and certifications associated with them do. Further, instructors often have educational reasons behind the timing for distribution of course materials, which could be undermined by this action. Content that is no longer available should not be shared nor used. If you believe that materials you have from a prior course might be useful for currently enrolled students, please contact the Chief Administrative Officer to suggest that it can be made available.

As a corollary, students should not receive previous materials from former or current students. Such materials may be incorrect or outdated.

Copyright violations are against US laws and international treaties, including but not limited to the Digital Millennium Copyright Act of 1998 and other US copyright laws (see www.copyright.gov/title17/)

For more information, please visit the U.S. Copyright Office website at www.copyright.gov, and their FAQ at www.copyright.gov/help/faq.

STUDENT CONDUCT

Students at Lab Four are expected to exhibit good manners and to conduct themselves as professionals preparing for responsible careers in the business world. Students should not interfere with the learning process of any other student, classroom presentation, or assignment of any instructor and should comply with all requests of an instructor or staff member relating to student conduct in the classroom or elsewhere on the school premises.

Students are obligated to comply with all local, state, and federal laws. When, at the discretion of a Lab Four staff member, a student is judged to be in violation of the Student Code of Conduct, appropriate action will be taken to restore and protect the normal functioning of the Lab Four learning habitat.

The Chief Administrative Officer will decide on all conduct violations. For re-admittance after a dismissal, students must demonstrate a sincere attitude toward learning, and the CAO may require an Academic Plan.

While it is impossible to determine all possible violations that might require disciplinary action, below is a good sampling of rules that Lab Four will enforce, including up to immediate termination without refund and, if necessary, legal action.

Students must not:

- Violate any provisions of the Enrollment Agreement, policies set forth in this Student Handbook, or any other Lab Four policies
- Remove any supplies, textbooks, equipment, or other property of Lab Four without written permission from the CAO
- Smoke anywhere inside the premises (smoking must be done outside at a reasonable distance from the front door)
- Use or possess any alcoholic beverages, narcotics, or controlled substances of any kind while on school grounds. Any extraordinary behavior that may be attributed to the use of drugs or alcoholic beverages shall not in any way limit the responsibility of the individual or the consequences of their actions.
- Enter the premises/grounds while in a state of intoxication
- Steal, vandalize, intentionally misuse, or willfully damage any Lab Four property, including Lab Four staff
- Act in a lewd or indecent way, including (but not limited to): sexually suggestive physical or verbal intentions, displaying obscene or libelous written or graphic materials while on Lab Four grounds (however briefly)
- Conduct any sort of mental or physical abuse of any person on Lab Four premises, including verbal or physical actions which threaten or endanger their health or safety
- Sexually suggestive or harassing verbal or physical behavior that in any way interferes with a student's or staff member's performance or creates an intimidating, hostile, or offensive environment
- Intentionally disrupt or prevent the teaching, research, administration, or disciplinary proceedings of Lab Four staff, or any other Lab Four activities, such as public service functions or any duly authorized activities occurring on Lab Four premises
- Conduct any unauthorized, un-prescribed, or non-customary use, occupation, or seizure of Lab Four property or any portion thereof
- Possess or use any firearm, knife, club, or other dangerous or deadly weapon, incendiary device, or explosive in connection with Lab Four approved activities or on the premises
- Use or tamper with any fire safety equipment or alarm except with reasonable belief of the need for such emergency equipment

- Gamble in any format, including wagering online
- Forge, alter, or misuse Lab Four documents, records, or identification instruments with reasonable intent to deceive
- Fail to pay for educational services rendered, including passing a worthless check
- Violation of a local, state, or federal law while on Lab Four premises

Student Internet Acceptable Use Policy

Lab Four provides Internet access to students to assist them in carrying out their duties for Lab Four. The internet may only be accessed by using the company's content scanning software, firewall and router.

Purpose

The purpose of this policy is to define standards and help the student make the best use of the Internet resources provided by Lab Four. These standards are designed to ensure students use the Internet in a safe and responsible manner.

Scope

This policy applies to all personnel, students, contractors and vendors with Internet access.

Internet Dos

- Do keep your use of the Internet to a minimum
- Do check that any information you access on the Internet is accurate, complete and current
- Do respect the legal protections to data and software provided by licenses
- Do inform the IT Department immediately of any unusual occurrence

Internet Don'ts

- Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity
- Do not download content from Internet sites unless it is school related and approved by the IT Department
- Do not download software from Internet sites and install it on Lab Four's computers
- Do not use Lab Four's computers to make unauthorized entry into any other computers or networks
- Do not access personal, dating, intimate apparel, gambling, or gaming sites
- Do not use Internet access to transmit political, obscene, threatening or harassing materials

Website Monitoring

Internet activity from all computers and devices connected to Lab Four's network is capable of being monitored, logged and scanned for offensive material. Social media sites (i.e. Facebook, Twitter, and Instagram) should only be accessed for business purposes.

Enforcement

Any student found to have violated these policies may be subject to disciplinary action, up to and including termination of enrollment.

DRUG AND ALCOHOL PREVENTION POLICY, TOBACCO USE, CLERY ACT, AND VAWA

Tobacco use of any kind (cigarette, 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.

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. Lab Four 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
- Falsifying student records, including attendance records or graded assignments
- Unsatisfactory Academic Progress, or failure to resolve a SAP/EEAS Hold as defined in the Satisfactory Academic Progress Policy
- Failure to attend for 14 consecutive calendar days
- Failure to attend at least 80% of the clock hours expected to date at the program midpoint
- Nonpayment of any student loan or other financial obligation

CONDITIONS FOR READMISSION

If a student wants to reenter who is dismissed from the program for academic or attendance-related reasons, they must go through the enrollment process. Approval for reenrollment is at the sole discretion of Lab Four.

Some violations are considered serious enough that a single offense could result in immediate dismissal. For a less serious offense, the Director will discuss the matter with the student in an effort to resolve the problem. Documentation of the violation will be put into the student's file. Notification of suspension will be in writing and will include a date, after which the student may apply for readmission. The student may be readmitted at such time as an opening exists.

COURSE COMPLETION REQUIREMENTS

1. Students must maintain adequate attendance according to published Attendance Policy (minimum 80%).
2. Students must complete all required academic assessments, maintaining an average course grade of 70% or higher.

GRADING SCALE

The following is the grading scale based on the percentage of points earned over the length of a program or course. A "passing" score is considered to be a "C" average or higher; or a cumulative grade percentage of 70% or higher.

% of Total Points Earned	Letter Grade
90-100	A
80-89	B
70-79	C
60-69	D
59 or Below	F
Temporary Leave of Absence	L

Vocational Clock Hour Programs

The final program grade will be comprised of several different components, each critical to the success of the student. The following table is a sample demonstrating the weight or percentage of the total grade assigned to various components:

Criteria	% of Total Grade
Post Assessments	30%
Practice Tests	20%
Hands-On Activities	20%
Final Exam	20%
Class Participation	10%

A student must achieve the following to graduate from a **clock hour** program at Lab Four:

- Cumulative grade percentage of 70% or higher
- Completion of 80% of the scheduled clock hours
- Completion of the graduation requirements within the maximum time frame, which is 150% of the published length of the program or up to a maximum of 15 weeks beyond the published program end date, whichever is shorter.

SATISFACTORY ACADEMIC PROGRESS

Quantitative progress is based on the completion of clock hours. Students must complete 80% (minimum) of the scheduled clock hours for their program. Attendance is monitored by the Instructor and SAP Compliance Team. Qualitative progress is based upon the cumulative grade percentage. The minimum cumulative grade percentage required is 70%.

Students must be progressing at a rate at which would allow them to complete their program within the maximum time frame, which is 150% of the published length of the program or up to a maximum of 15 weeks beyond the published program end date, whichever is shorter. The end of this time frame for each class is known as the Academic Deadline.

Each class's Academic Progress is evaluated weekly, or no less frequently than at completion of 25%, 50%, 75%, and 100% of the class schedule to ensure that students are on track to pass the course. This evaluation includes the cumulative grade percentage and the attendance rate in percentage form. Each student is provided this evaluation (of their individual performance) electronically via the Student Portal. Electronic records of attendance logs and grades contributing to the cumulative grade percentage and attendance rate for each student are also placed in the appropriate class file.

If a student fails to meet the cumulative 80% attendance or 70% cumulative grade percentage for any evaluation period, or both, they are placed in warning status for the next evaluation period and may be subject to a Corrective Action Plan to regain Satisfactory Academic Progress. Students' eligibility for scholarships and grants is not affected while on warning status, as long as the student remains enrolled, unless specifically stated by the scholarship or grant provider. Failure to achieve SAP standards at the end of the warning period will result in the administrative withdrawal of the student.

Students will be notified via email if they are in warning status and the steps necessary to be removed from warning status, or if they are administratively withdrawn, and documentation will be stored in the SAP Documentation Repository.

Incomplete grades are not given, and students must repeat any classes in which they do not meet completion requirements. Students who withdraw from the program will receive a failing grade in each class interrupted by the withdrawal. All interrupted classes must be repeated upon re-admission into Lab Four.

Students in violation of Lab Four's Satisfactory Academic Progress, Attendance, or Student Conduct policies at any point during the program are not considered eligible to receive Employment and Entrepreneurship Assistance Services (EEAS) until such issues are resolved. Those who have not met the course completion requirements detailed above will be subject to a *SAP Hold*. This prevents them from progressing to the next module within their program (if applicable); as well as from enrolling in additional programs unless the hold is resolved. Students prevented from progressing from one module to the next within their program as the result of a SAP Hold will be administratively withdrawn from the program.

Students enrolled in vocational programs who do not engage with the EEAS department to actively work toward meaningful employment outcomes per the guidelines provided in the course syllabus will be subject to an *EEAS Hold.* Like with a SAP Hold, Students with an EEAS Hold are prevented from progressing from one module to the next within their program (if applicable); as well as from enrolling in additional programs unless the hold is resolved. Students prevented from progressing from one module to the next within their program as the result of an EEAS Hold will be administratively withdrawn from the program.

APPEAL PROCESS

Students terminated (withdrawn) from Lab Four will be notified via email of their dismissal. To appeal a termination, the student must submit a written appeal (email is an accepted form of written communication) to the Campus Director via help@labfour.edu within 10 days of the dismissal notification. Appeals may be granted for mitigating circumstances defined as; documented student illness or 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 student's written appeal must include a detailed statement defining the mitigating circumstances that contributed to the student's failure to meet Satisfactory Academic Progress, Attendance, or Student Conduct standards and what has changed in the student's situation that will allow them to meet these standards at the next SAP evaluation, and going forward through the end of their program.

Students that have submitted an appeal will not be considered terminated until a decision to approve or deny the appeal is made by the Appeals Committee. Students are therefore expected to attend training during the appeal process and are responsible for attending all scheduled class sessions and submitting all graded assignments due within the appeal time frame. Before an appeal may be granted, a written academic plan must be provided to the student, which clearly identifies a viable plan for the student to successfully complete the program within the maximum time frame allowed. Lab Four will recognize an automatic request for appeal for a 14 consecutive day absence if a student's last day of attendance is within 24 days from their scheduled graduation date and they have met all graduation requirements.

The Appeals Committee, composed of the Campus Director and Academic Director, 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 committee. The student will be sent the committee's decision within 30 days of the Campus Directors receipt of the appeal.

The committee's decision is final. The withdrawal calculation for students whose appeal is denied is based on their last day of attendance.

TRANSFER STUDENTS

Students awarded transfer credit will have their enrollment term adjusted based on the number of clock hours remaining. Transfer hours will be counted toward the maximum time frame. Attendance and academic progress will be evaluated at the regular scheduled intervals per the Satisfactory Academic Progress Policy and the prorated program maximum time frame (150% of the hours completed at this institution). Qualitative and quantitative measures will be based only on credits earned at Lab Four.

CONFIDENTIALITY OF STUDENT RECORDS

The policy of Lab Four 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 their education records within 45 days of the day the school receives a request for access; the right to request an amendment of their education records that the student believes are inaccurate or misleading; the right to consent to disclosures of personal identifiable information (PII) contained in their 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 Lab Four 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.

CLOCK HOUR AND CREDIT HOUR POLICY

All certificate programs at Lab Four are measured in clock hours only. A clock hour is defined as a 60-minute span of time, with no less than 50 minutes of actual class instruction. Degree programs are measured in both clock hours and quarter credit hours. Lab Four uses the following clock-to-credit hour conversion formula for academic purposes:

Lecture Hours: Instructional hours consisting of theory or new principles
Lecture Credit Hours (Quarter Credit Hours): Must teach at least 10 lecture hours to award 1 quarter credit (divide lecture hours by 10)

Laboratory Hours: Instructional hours consisting of supervised student practice of a previously introduced theory/principle during which practical skills and knowledge are developed and reinforced
Laboratory Credit Hours (Quarter Credit Horus): Must teach at least 20 laboratory hours to award 1 quarter credit (divide laboratory hours by 20)

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 Registration Specialist via help@labfour.edu. There is no transcript release fee at this time.

EVALUATION OF INSTRUCTORS

All students will be asked to evaluate their instructors and their overall experience with Lab Four. Evaluations are conducted at the midpoint and endpoint of each cohort. These surveys provide Lab Four with valuable input for improvement.

TUITION PAYMENT

All students are required to secure funding and/or commit to a written loan or payment plan contract for the full balance of tuition and course materials fees, as applicable, prior to the start of the first class session of each payment period or period of financial obligation.

For certificate programs with a scheduled duration shorter than 12 months, students are subject to a single period of financial obligation matching the full length of the program in weeks. For Occupational Associate Degree (OAD) programs, which have a scheduled duration of seven 10.5-week quarters over an 18-month or two-year academic period; each 10.5-week quarter represents a separate period of financial obligation. Refund computations are applied according to the stated charges attributable to the relevant period of financial obligation based on the last date of attendance (LDA).

Lab Four accepts tuition payment in the form of a cashier's check, money order, credit card, grant or scholarship approval, or student loans where available.

Lab Four also accepts WIOA, SNAP-ET, and other grant vouchers as detailed in the Financial Aid section below. Tuition payment must be arranged or received prior to enrollment. 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 your Career Specialist or Financial Aid Specialist if you don't seek private lending on your own. For more information about private lending options please contact your Career Specialist. Lab Four 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.

If payment or funding approval is delayed beyond the Registration Deadline, students will be placed on the roster for the next cohort of the same program and will be given a new start date upon receipt of payment or funding approval. In the event the student defaults on their bill, the account may be sent to collections and the student will be liable for any collection charges and/or legal fees incurred on their account.

Additionally, students are subject to termination for nonpayment. Lab Four 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 below. Lab Four will also charge a $50.00 service fee for any returned checks that are given to the school as payment for tuition.

Students who do not officially withdraw from classes on or prior to the official start date will be responsible for any tuition and fee charges incurred, according to the published Refund and Cancellation Policy.

Students who are able to secure funding for 100% of the tuition and fees associated with their program(s) from sources such as WIOA, SNAP-ET, community grants or scholarships may begin class upon Lab Four's receipt of the final funding approval, provided the student's application packet is complete and accepted.

In the event that a student's tuition and fees are not covered in full by a grant, scholarship, or education benefit, the student is responsible for the remaining balance of tuition and course materials fees associated with the program. The remaining balance can either be paid up front, in full, or the student must commit to a written loan or payment plan option prior to enrollment.

Payment plan options are detailed in the Financial Aid section below.

Certification Exam Payment

Lab Four will not pay for any certification exam attempt for a student with an outstanding balance. Certification exam costs are not included in the tuition and fees. Students enrolled in a payment plan are responsible for the cost of any certification exams they wish to take.

All students are informed of the cost of the certification exam(s) associated with their program prior to enrollment.

FINANCIAL AID

Students may qualify for the following grants and financial assistance. This information is subject to change based on governing agencies' policies or additional sources made available. To learn more about any option listed below, contact your Career Specialist or our Financial Aid Department.

Loyalty Scholarship

Lab Four offers a Loyalty Scholarship to any returning student who has successfully completed a training program with us in the past. This is a $750 tuition discount on an 8-week program, or a $2,500 tuition discount on a 30-week program. To qualify, applicants must meet the following criteria:

1. Must have met program completion criteria for at least one previous enrollment – at minimum, 80% final attendance rate and 70% final cumulative grade
2. Must not have any outstanding financial balance or documentation owed to Lab Four
3. Must be self-funded for the enrollment to which the scholarship is applied (payment plan or up-front payment)

The Loyalty Scholarship is not combinable with any other scholarship or grant option.

Each year, we also provide a limited number of full scholarships (covering 100% of tuition and course materials fees) to select graduates based on their performance during previous enrollment(s) at Lab Four. Participants are selected based on grades and attendance, class participation, engagement with Employment and Entrepreneurship Assistance Services (EEAS), achievement of training-related placement outcomes and/or industry certification attainment, and instructor recommendations – as well as the dedication and enthusiasm shown toward pursuing careers in the tech field.

Loyalty Scholarship recipients are responsible for the cost of any industry certification exams they wish to take. They are not eligible for exam vouchers from Lab Four.

Financing Options

Lab Four offers a tuition financing option through Fortify. This option requires a minimal down payment (typically less than 10% of the tuition cost) prior to the start of class. The student is responsible for the full tuition and course materials fee balance, plus a servicing fee. Payment terms and monthly payments vary according to the total program cost, down payment amount, and the student's state of residence, however monthly payments are generally kept between **$250.00 – 300.00 per month**.

The first payment of your Fortify payment plan is due 30 days after your class start date.

Students who receive a grant voucher that will cover a portion of their tuition and fees, but still have a remaining balance, may **use their grant voucher as their down payment** if they wish to apply for a Fortify loan to finance the remaining balance.

Please note that grant participants who fail to meet program completion requirements forfeit eligibility for the grant funding. In the event of withdrawal, the student is liable for the tuition and course materials fees assessed as of the last date of recorded attendance, subject to Lab Four's Refund and Cancelation Policy.

Employer Reimbursement

You may have financial aid options available through your employer. Tuition reimbursement benefits are often not widely or enthusiastically promoted. Typically, tuition assistance is based upon an employer's objectives for recruiting, retention, and productivity. Benefits vary from company to company, and even within various divisions of the same company. Make an appointment to speak with your Human Resources specialist about your employer's rules and restrictions. You may also be able to find information in your Employee Handbook.

Conditional Government Grant Options

Government grants may be available to those who meet eligibility requirements. Approval is not guaranteed and the application process may take up to 2-3 months.

- **Workforce Innovation and Opportunity Act (WIOA)**
  WIOA is the 2014 amendment and reauthorization of the Workforce Investment Act (WIA) of 1998. WIOA is designed to help job seekers access employment, education, training, and support services needed to succeed in the labor market and to match employers with the skilled workers they need to compete in the global economy. WIOA grants typically target dislocated workers, and low-income, unemployed, or underemployed individuals who have obtained their High School Diploma or equivalent.

- **Supplemental Nutrition Assistance Program Employment and Training (SNAP-ET)**
  This program is designed to help eligible participants (those receiving SNAP benefits) to achieve their vocational goals and increase self-sufficiency through funded education, skills training, and supportive services.

Other Grants and Community Organizations
Lab Four has worked with several local community organizations dedicated to supporting and improving the lives of young adults, low-income individuals, and Veterans transitioning out of military service and into civilian life in Middle and West Tennessee. Many of these organizations include funding for education and training among the supportive services they offer.

We are also part of a consortium that has been awarded over $40 million in grant funding from the US Department of Labor since 2011, to provide technical training and employment and entrepreneurship assistance in West Tennessee and the surrounding area.

For more information, please contact our Financial Aid Department.

CERTIFICATION EXAMS

All of Lab Four's programs are aligned with and designed to help students obtain industry certifications. These certification exams are optional, but students are strongly encouraged to take them. Certifications validate the holder's skillset and experience and serve as an indication of an individual's work ethic, learning ability, and career focus to employers. Lab Four offers all of its course content and various tools including practice tests, practice labs, and summaries of exam objectives as provided by vendors like Microsoft, Cisco, and CompTIA to help prepare students to pass the certification exams associated with their program.

GRIEVANCE PROCEDURE

If a student has a complaint or grievance of any kind, they must first speak to their instructor one-on-one (not during class). If unsatisfied with the results of the meeting with their instructor, students should contact the Concerns Committee by emailing help@labfour.edu. If still unsatisfied, students are encouraged to contact the Campus Director so that Lab Four can work to resolve the issue. If a student has a grievance that has not been resolved with the Campus Director, the student may submit a written statement/report (U.S. mail or hand-delivery) describing the issue or complaint to the Director of Operations of Lab Four, 1255 Lynnfield Road, Suite 160, Memphis TN 38119. Telephone: 901-261-1111. The Director of Operations will review the statement, may meet with the student, and will respond within ten days. The decision of the Director of Operations is final.

Discrimination complaints must be filed no later than 180 days after an alleged discrimination. At each step of our process, hearings are held within 30 days of filing the grievance, with a decision made no later than 60 days after filing.

If a student does not feel that the school has adequately addressed a complaint or concern after exhausting the school's procedures, the student may contact the Tennessee Higher Education Commission, 312 Rosa Parks Ave, 9th Floor, Nashville, TN 37243. Telephone: 615-741-3605

If the student is a WIA or WIOA participant, they have the right to request a review by the Governor within 10 days of receipt of the adverse decision or from the date on which they should have received a decision. Telephone: 615-741-2001.If the student is part of a program involving an employer/contractor, the employer/contractor's decisions can be reviewed by LWIA and the Governor if necessary. If necessary, the student may also contact the Department of Labor at 615-741-1031.

After exhausting institutional procedures, students may contact ACCET (see below).

NOTICE TO STUDENTS: ACCET COMPLAINT PROCEDURE
This institution is recognized by the Accrediting Council for Continuing Education & Training (ACCET) as meeting and maintaining certain standards of quality. It is the mutual goal of ACCET and the institution to ensure that quality educational training programs are provided. When issues or problems arise, students should make every attempt to find a fair and reasonable solution through the institution's internal complaint procedure, which is required of ACCET-accredited institutions and frequently requires the submission of a written complaint. Refer to the institution's written complaint procedure, which is published in the institution's catalog or otherwise available from the institution, upon request. Note that ACCET will process complaints that involve ACCET standards and policies and, therefore, are within the scope of the accrediting agency.

If a student has used the institution's formal student complaint procedure, and the issue has not been resolved, the student has the right and is encouraged to submit a complaint to ACCET in writing via the online form on the ACCET website (https://accet.org/about-us/contact-us). The online form will require the following information:

1. Name and location of the ACCET institution
2. A detailed description of the alleged problem(s)
3. The approximate date(s) that the problem(s) occurred
4. The names and titles/positions of all persons involved in the problem(s), including faculty, staff, and/or other students

5. What was previously done to resolve the complaint, along with evidence demonstrating that the institution's complaint procedure was followed prior to contacting ACCET
6. The name, email address, telephone number, and mailing address of the complainant. If the complainant specifically requests that anonymity be maintained, ACCET will not reveal his or her name to the institution involved
7. The status of the complainant with the institution (e.g., current student, former student)

Please include copies of any relevant supporting documentation (e.g., student's enrollment agreement, syllabus or course outline, correspondence between the student and the institution).

Note: Complainants will receive an acknowledgment of receipt within 15 business days.

Online Complaint Submission Form

National Council for State Authorization Reciprocity Agreement (NC-SARA) Student Complaint Process
Cybersecurity Institute at Lab Four Complaint Policies for Certain Distance Education Students Enrolled Through the State Authorization Reciprocity Agreements ("SARA")

The below policies apply to students who are:

- non-Tennessee residents in State Authorization Reciprocity Agreement ("SARA") states and who are enrolled in a distance education program/course or
- attending an out-of-state learning placement in a SARA state other than Tennessee

The nature of complaints to be addressed through these policies include violations of SARA policies and dishonest or fraudulent activity. These policies do not apply to complaints concerning student grades or student conduct violations. For more information on complaint subject matter see *SARA Policy Manual* Sections 4.2 and 4.3.

Institution Complaint Policies are listed above, under **GRIEVANCE PROCEDURES** beginning on **page 17** of this handbook.

Additional Complaint Policies:

- Tennessee Higher Education Commission ("THEC")
    - Students (as described above) must complete the institution complaint process before appealing to THEC.
    - Students who are not satisfied with the institution's resolution of their complaint may appeal the institution decision to THEC using the Request for Complaint Review form. Additional information on the THEC complaint process is available at THEC Complaint Review Process. Students may also contact THEC.RCD@tn.gov with questions.
    - The appeal to THEC must be filed within two (2) years of the incident about which the complaint is made.
    - Out-of-state student may also contact their home state higher education authority; although student may be referred to THEC. See State Portal Entity Contacts | NC-SARA for a listing of SARA states and contacts.
    - Students residing in non-SARA states, currently California only, should consult their respective state of residence for further instructions for filing a complaint.
    - Any person claiming damage or loss as a result of any act or practice by an authorized postsecondary educational institution or its agent that is a violation of Title 49, Chapter 7, Part 20 or Rule Chapters 1540-01-02 or 1540-01-10, may file a complaint with THEC after exhausting the institution complaint process. More information is available at THEC Complaint Review Process, 312 Rosa Parks Ave., 9th Floor, Nashville, TN, 37243, (615) 741-3605. Students may also contact THEC.RCD@tn.gov with questions.

NON-DISCRIMINATION AND HARASSMENT POLICY

Lab Four intends to provide an academic and working environment that is free from discrimination, intimidation, hostility, or harassment, which might interfere with the work of employees or the experiences of students in the program. Harassment of any sort – verbal, physical, visual, or electronic – will not be tolerated. If you become aware of any instances of harassment at Lab Four, notify Lab Four management immediately.

WHAT IS HARASSMENT?

Harassment includes, but is not limited to inappropriate or offensive words, signs, jokes, pranks, intimidation, or physical contact that is based on race, color, sex, religion, national origin, age, disability, or sexual preference. Sexual harassment occurs when any supervisor, or other employee, threatens or insinuates, directly or indirectly, that an employee's or student's submission to, or rejection of, unwelcome sexual conduct will affect the employee's job, evaluation, assigned duties, compensation, or any other term or condition of employment, or the student's participation, advancement, or academic standing in our educational program.

Sexual harassment may also occur when unwelcome sexual advances, requests for sexual favors, or any other verbal or physical conduct or activity of a sexual nature is so severe, persistent, or pervasive as to affect the ability of an employee to perform his or her job, or the ability of a student to fully participate in our education program, or when such activity creates an intimidating, hostile or offensive work or learning environment.

All students and employees, full and part-time, have a responsibility for keeping Lab Four free of harassment.

STATE OF TENNESSEE REFUND AND CANCELLATION POLICY

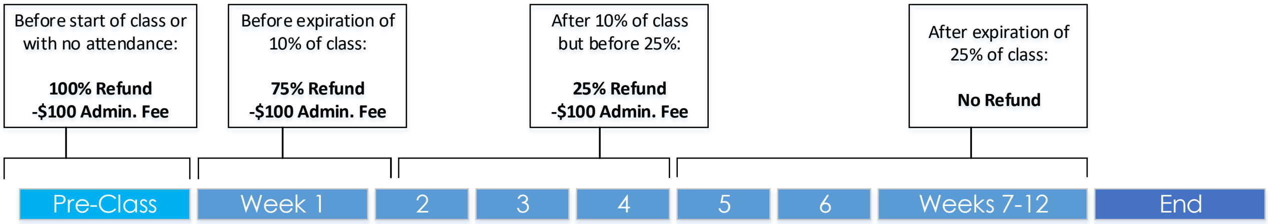
Refund procedure before entering class:

1) You will receive a full refund of all money paid if you are not accepted by the school.
2) You will receive a full refund of tuition paid minus a $100 non-refundable administrative fee if you withdraw prior to the start date of class or never once attend class.
3) If Lab Four cancels a program subsequent to a student's enrollment, Lab Four will refund all monies paid by the student.

Refund procedure after entering class:

1) If a student withdraws from the institution on or before the first day of classes, or fails to begin classes, the refund shall equal the sum of all amounts paid or to be paid by or on behalf of the student for the period of enrollment, less an administrative fee of one hundred dollars ($100.00);
2) If after classes have commenced and before expiration of ten percent (10%) of the period of enrollment for which he or she was charged, a student withdraws, drops out, is expelled, or otherwise fails to attend classes, the refund shall equal seventy-five percent (75%) of all amounts paid or to be paid by or on behalf of the student for the period, less administrative fee of one hundred dollars ($100.00);
3) If after expiration of the of ten percent (10%) of the period of enrollment for which he or she was charged, and before expiration of twenty-five percent (25%) of the period, a student withdraws, drops out, is expelled, or otherwise fails to attend classes, the refund shall equal twenty-five percent (25%) of all amounts paid or to be paid by or on behalf of the student for the period, less administrative fee of one hundred dollars ($100.00);
4) If after expiration of twenty-five (25%) of the period of enrollment for which he or she was charged, a student withdraws, drops out, is expelled, or otherwise fails to attend classes, the student may be deemed obligated for one hundred (100%) of the tuition, fees and other charges assessed by the institution.

The following chart illustrates our policy:
Example given is for a 12-week class.



Before start of class or with no attendance:
100% Refund
-$100 Admin. Fee

Before expiration of 10% of class:
75% Refund
-$100 Admin. Fee

After 10% of class but before 25%:
25% Refund
-$100 Admin. Fee

After expiration of 25% of class:
No Refund

Withdrawals/Drops:

Unless otherwise noted above, the official date of termination of a student shall be the last date of recorded attendance. Withdrawal occurs in any of the following manners: 1) When the school receives notice of the student's intention to discontinue the training, 2) When the student is terminated for violation of a published school policy which provides for termination or 3) When a student, without notice to the institution, fails to attend classes for thirty (30) calendar days.

Exception:

All or a portion of the tuition, fees, and other institutional charges assessed the student were paid or to be paid by student assistance programs sponsored by one or more governmental or private agencies or organization, including employer provided financial assistance, and the institution, as a condition of establishing eligibility for its students to participate in such programs, is required to adhere to a refund policy prescribed by the sponsor of the student assistance. In the event of this exception, the refund policy required by that organization shall be adhered to.

ACCET REFUND AND CANCELLATION POLICY

For certificate programs with a scheduled duration shorter than 12 months, students are subject to a single period of financial obligation matching the full length of the program in weeks. The tuition and fees associated with each certificate program are specified in Lab Four's Student Handbook and Catalog, as well as on the Enrollment Agreement for each student enrolled.

For Occupational Associate Degree (OAD) programs, which have a scheduled duration of seven 10.5-week quarters over an 18-month or two-year academic period; each 10.5-week quarter represents a separate period of financial obligation. The tuition and fees associated with each 10.5-week quarter are specified in Lab Four's Student Handbook and Catalog, as well as on the Enrollment Agreement for each student enrolled in the OAD program.

Refund computations are applied according to the stated charges attributable to the relevant period of financial obligation based on the last date of attendance (LDA).

Refund procedure <u>before</u> entering class:

1) You will receive a full refund of all money paid if:
   a. You are not accepted by Lab Four.
   b. You withdraw on or prior to the start date of class or never once attend class (no-show).
   c. Lab Four cancels a program after your enrollment.
2) If a student never attends class (no-show) or cancels the contract prior to the class start date, all refunds due will be made within forty-five (45) calendar days of the first scheduled day of class or the date of cancellation, whichever is earlier.

Refund procedure <u>after</u> entering class:

1) During the first week of classes, tuition charges withheld will not exceed 10% of the stated tuition up to a maximum of $1,000.
2) Refund amounts are based on the student's last date of attendance (LDA). When determining the number of weeks completed by the student, Lab Four 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) For students in residential programs, the LDA is the last date of recorded attendance in the classroom.
   b) For students in IDL programs, the LDA is the last date academic work was completed – this could be either attendance in a live, interactive class session; or completion of a lab or homework assignment, whichever is later.
3) After the first week and through 50% of the period of financial obligation, tuition charges retained will not exceed a pro rata portion of tuition for the training period completed plus an administrative fee of one hundred dollars ($100.00).
4) After 50% of the period of financial obligation is completed, the institution may retain the full tuition.
5) For any student withdrawn or terminated after entering class, all due refunds shall be made within forty-five (45) days after the date of determination.
6) For an enrolled student, the refund due will be calculated using the last date of attendance (LDA) and be paid within forty-five (45) calendar days from the documented date of determination (DOD). The DOD is the date the student gives written or verbal notice of withdrawal to the Lab Four or the date that Lab Four terminates the student, by applying Lab Four's attendance, conduct, or Satisfactory Academic Progress policy. If a student provides advanced notice of withdrawal such that the 45-day window for refund processing ends before the last date of attendance, the refund must be paid within forty-five (45) calendar days from the LDA.

Charges Other Than Tuition:

After entering class, all extra costs such as books, supplies, equipment, laboratory fees, rentals and any similar charges not included in the tuition price are not subject to refund. Such charges are identified as nonrefundable in both the Catalog and Enrollment Agreement. Charges that are non-refundable must be limited to those materials that are distributed and attributable to the portion of the program attended by the student.

Withdrawals/Drops:

Withdrawal occurs in any of the following manners: 1) When the school receives notice of the student's intention to discontinue the training, 2) When the student is terminated for violation of a published school policy which provides for termination or 3) When a student, without notice to the institution, fails to attend classes for fourteen (14) calendar days.

Since ACCET and the Tennessee Higher Education Commission have different refund policies, both policies will be applied at the time of withdrawal to calculate refund eligibility. Lab Four will apply whichever refund is more lenient to the individual student.

EMPLOYMENT AND ENTREPRENEURSHIP ASSISTANCE SERVICES (STUDENT/CAREER SERVICES)

The mission of Lab Four's Employment and Entrepreneurship Assistance Services (EEAS) department is to assist students and alumni in achieving their career goals. To this end, EEAS seeks to:

- Provide students/alumni with the tools, instruction, and encouragement to interface with future employers
- Work with employers to cultivate the best opportunities for students and alumni
- Partner with the business community to promote career skills and opportunities for students and alumni

Services for Students

Employment and Entrepreneurship Assistance Services can provide a major advantage in the form of career development. We strive to provide every student with skills that will assist them in their lifelong career journey. The EEAS Department helps to get students on the path to developing their career with the following resources:

- One-on-one Career Counseling and Job Search Coaching with an EEAS Specialist
- One-on-one Resume and Cover Letter Assistance
- Resume, Technical Interview Skills, and Entrepreneurship Workshops
- Technical Mock Interviews
- Job Opportunity Notifications
- Refresher courses and extended access to course materials for alumni in good standing* up to one year after class completion
- On-Site Certification Testing Center

**For the purpose of this section, "alumni in good standing" refers to individuals who have met the course completion requirements identified on page 13 of this handbook; as well as achieved a training-related employment or entrepreneurship outcome complete with all required documentation for students enrolled in vocational programs. Additional requirements may apply for students participating in grant programs that include additional expected outcomes, such as certification attainment. Alumni who meet these qualifications may audit any class they completed for up to one year following their class completion date and receive extended access to course materials upon request*.

Regardless of where you are in your career planning, our counselors will assist in developing a plan to discover and reach your career goals. Obtaining employment in a training-related field is ultimately the responsibility of the student. Lab Four does not guarantee placement. Lab Four tracks the placement of its graduates for a minimum of 120 days after the class completion. Students in a program where self-employment is a common vocational goal will be asked to sign a Self-Employment Acknowledgement form during enrollment. Graduates will also be given the opportunity to waive placement services if they are not participating in a grant program for which placement is evaluated.

Students will be required to complete employment or entrepreneurship documentation as provided by Lab Four (via the Employment Verification Form), the government entity funding your training (if applicable), or both. Please be prepared to provide proof of meaningful employment in the form of an offer letter, pay stub, promotion offer, or a note from your manager. Business owners more specifically should be prepared to submit documentation of your Federal Tax ID/EIN; business license and registration; marketing material showing the scope or level or services offered; and one of the following: a business tax return, bank statements from the past six months showing self-employment income, or profit and loss statements. Students will be informed that their employer may be sent an Employer Satisfaction Survey to evaluate the performance of Lab Four graduates based on the knowledge acquired at Lab Four. Graduates may also be asked to sign employment satisfaction attestation forms as applicable depending on the type of job placement.

A graduate shall be considered "non-responsive" if they fail or refuse to communicate with EEAS Specialists (e.g. does not answer or return phone calls, does not return emails, contact info is bad, etc.) consistently for 30 calendar days. **

***For the purpose of this section, "consistent" is defined as four (4) documented communication attempts without any response.*

A student shall also be considered non-responsive if they fail or refuse to submit any necessary written documentation required by any governing authorities. In certain situations (as judged by Senior Management), students may also be considered non-responsive if they are given adequate, documented service (such as notifications of openings, connection with employers, other services, etc.), but refuse to attend interviews, pursue openings, etc. In these circumstances, the EEAS Specialist must contact Senior Management for approval to consider the student/graduate non-responsive.

Students enrolled in vocational programs who do not engage with the EEAS department to actively work toward meaningful employment outcomes per the guidelines provided in the course syllabus will be subject to an *EEAS Hold*. Similar to a SAP Hold, Students with an EEAS Hold are prevented from progressing from one module to the next within their program (if applicable); as well as from enrolling in additional programs unless the hold is resolved. Students prevented from progressing from one module to the next within their program as the result of an EEAS Hold will be administratively withdrawn from the program.

If a student fails to retain employment long enough to be considered placed due to legal issues (such as harassment, violence, etc.), insubordination toward their supervisor, attendance issues, sleeping on the job, or circumstances reasonably under the student's control, the student may be considered ineligible for EEAS with Senior Management approval.

ADMINISTRATIVE STAFF

Stephanie Okhiria (Executive Director and Chief Administrative Officer)
Tony Okhiria (Program Chair, Academic Manager, and Senior Advisor)
Lizz McDonough (Director of Compliance and Grants)
Brendan Wade (Technology Administrator)
Blessing Osasumwen (Administrative Assistant)

FACULTY

Tony Okhiria: Information Technology Classes; BS in Mathematics and Computer Science; MBA Information Systems: PhD Information Systems (ABD) (in progress); Certifications: MCSA, CCNA, CCNP, CCSI, CAPM, PMP, ITIL, DCI, MCSE, AWS.
Brandon Jackson: Information Technology Classes; AS Software Development; BS Information Security (in progress); Certifications: MCITP, MCTS, MCSA, MOS Excel 2013
Brendan Wade: Information Technology and Business Skills Classes; BS in Business Information Technology; Certifications: MCSA, MOS (Word, Excel, Outlook, and PowerPoint 2016)
Saul Mbenga: Adjunct Instructor, Information Technology; BS Computer Sciences, MBA Information Technology; Certifications: CCNA, CCDP, MCTS, MCDBA, MCITP, PMP, PMI-RMP
Carolyn Lanton: Adjunct Instructor, Information Technology and Business Skills; BS Management Information Systems; MBA Management; Certifications: PMP, Six Sigma Black Belt, ScrumMaster, ITIL, CCNA
JC Scott: Adjunct Instructor, Information Technology; AAS Information Technology; Certifications: CCNA
Quinton Harrison: Adjunct Instructor, Information Technology; Certifications: MCP, MCITP, ITIL, CCNA
Sheriff Toritsemotse: Adjunct Instructor, Information Technology; Certifications: CompTIA A+, Amazon AWS Certified Cloud Practitioner

CONTACT INFORMATION

1255 Lynnfield Road, Suite 160
Memphis, TN 38119
Phone: (901) 261-1111
Fax: (901) 261-1155
www.labfour.com

Instagram: @cyberseclabfour
X (Twitter): @cyberseclabfour
Facebook: facebook.com/cyberseclabfour
LinkedIn: linkedin.com/company/cyberseclabfour
YouTube: youtube.com/@cyberseclabfour

School policies are subject to change with Senior Management Approval.

Lab Four is an equal opportunity employer. All qualified applicants will be considered without regard for race, color, religion, sex, age, national origin, disability, sexual orientation, marital status, citizenship or other protected criteria.

DEGREE PROGRAMS

The programs included in this section are degree-seeking programs and are designed to provide our students with general education as well as better career opportunities according to industry demand.

If you have questions about any of these programs, please do not hesitate to contact your Career Specialist.

Please note that not all classes may always be available.

Cloud Security

Degree Program

Program Description

The Associate of Applied Science in Cloud Security program is designed to help students gain the knowledge and skills necessary to be confident and ready to work in the Information Technology field at the professional level.

Students will gain security and risk management skills that are among the most highly sought-after skills in networking. Additionally, completers will have hands-on knowledge of server configuration, client connectivity, security, networking, Active Directory, DNS, DHCP, troubleshooting, optimization and backup/recovery of critical data.

Courses include preparation for industry standard certifications CompTIA IT Fundamentals, CompTIA A+, Microsoft 365 Certified Fundamentals, Microsoft Certified Azure Fundamentals, (ISC)^2 Certified in Cybersecurity, Microsoft 365 Certified Endpoint Administrator Associate, Cisco Certified Support Technician (CCST) Networking, Cisco Certified Network Associate (CCNA), CompTIA Network+, CompTIA Security+, Cisco Cybersecurity Associate, Microsoft Certified Azure Administrator Associate, Microsoft Certified Information Security Administrator Associate, Cisco Certified Network Professional (CCNP) Enterprise, Amazon AWS Certified Cloud Practitioner, Amazon AWS Certified Solutions Architect – Associate, Ethical Hacker, Microsoft Certified Security, Compliance, and Identify Fundamentals, Systems Security Certified Professional (SSCP), Certified Information Systems Security Professional (CISSP), Certified Associate in Project Management (CAPM), Project Management Professional (PMP), Amazon AWS Certified SysOps Administrator – Associate, and Information Technology Infrastructure Library (ITIL) Foundation. Classes meet in state-of-the-art computer labs that offer the latest in networking technology.

This program totals 111 quarter credit hours, or 1,450 total contact hours. The program consists of seven 10.5-week quarters and takes place over a period of 2 academic years. Classes are offered in the daytime Monday through Thursday from 9:30am until 2:30pm; or in the evening Monday through Thursday from 5:30pm until 10:30pm. Students must complete all the courses listed below:

		Quarter Credit Hours			Contact (Clock) Hours			Homework (outside of class hours)
Quarter	Required Courses	Lecture	Lab	Total Hours	Lecture	Lab	Total Hours	
1	**Introduction to Communication**	3	1	4	30	20	50	10
	Operating Systems I	4	2	6	40	40	80	15
	Cloud Security Foundations	4	2	6	40	40	80	15
	Quarter 1 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
2	**English Composition I**	3	1	4	30	20	50	10
	Client	4	2	6	40	40	80	15
	Networking I	4	2	6	40	40	80	15
	Quarter 2 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
3	**Critical Thinking and Logic**	3	1	4	30	20	50	10
	Security I	4	2	6	40	40	80	15
	Networking II	4	2	6	40	40	80	15
	Quarter 3 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
4	**Communication and Customer Relations**	3	1	4	30	20	50	10
	Cloud Security I	4	2	6	40	40	80	15
	Networking and Security III	4	2	6	40	40	80	15
	Quarter 4 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
5	**Employment Preparation**	3	1	4	30	20	50	10
	Networking IV	4	2	6	40	40	80	15
	Cloud Security II	4	2	6	40	40	80	15
	Quarter 5 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
6	**Group Dynamics**	3	1	4	30	20	50	10
	Security II	4	2	6	40	40	80	15
	Security III	4	2	6	40	40	80	15
	Quarter 6 Total:	**11**	**5**	**16**	**110**	**100**	**210**	**40**
7	Project Management	4	2	6	40	40	80	15
	Cloud Security III	4	2	6	40	40	80	15
	ITIL Foundation	3	0	3	30	0	30	10
	Quarter 7 Total:	**11**	**4**	**15**	**110**	**80**	**190**	**40**
		Quarter Credit Hours			**Contact (Clock) Hours**			**Total Homework Hours:**
		Lecture	**Lab**	**Total Hours**	**Lecture**	**Lab**	**Total Hours**	
	Program Total:	**77**	**34**	**111**	**770**	**680**	**1,450**	**280**

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program
Computer and Information Systems Manager, Computer Network Architect, Information Security Analyst, Network and Computer Systems Administrator, Help Desk Support, IT Support Specialist, Network Technician, Network Administrator, Information Security Administrator, Network Operation Technician, Network Support, Computer Support Specialist, Desktop Support, Web Developer, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Associate of Applied Science
Length of Program:	111 Quarter Credit Hours (7 x 10.5-week quarters) 1,450 Clock Hours
Lecture/Lab Hours:	77/34 (measured in quarter credit hours)
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$37,050.00**
Course Materials Fee (nonrefundable):	**$6,775.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	*Tuition*	*Course Materials*	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Introduction to Communication	*$1,531.13*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Operating Systems I	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Security Foundations	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
English Composition I	*$1,531.14*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Client	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Networking I	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Critical Thinking and Logic	*$1,056.12*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Security I	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Networking II	*$2,451.10*	*$475.00*	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Communication and Customer Relations	*$1,531.13*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Cloud Security I	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking III	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Employment Preparation	*$1,056.12*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Networking IV	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Cloud Security II	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Group Dynamics	*$1,056.12*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*
Security II	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Security III	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Project Management	*$1,690.69*	*$250.00*	*$50.00*	*$100.00*	*$75.00*	*$25.00*
Cloud Security III	*$1,690.69*	*$500.00*	*$150.00*	*$225.00*	*$100.00*	*$25.00*
ITIL Foundation	*$1,056.12*	*$175.00*	*$25.00*	*$50.00*	*$75.00*	*$25.00*
TOTAL:	*$37,050.00*	*$6,775.00*				

The program tuition and fee breakdown *by quarter* is as follows:

Program Cost	**$43,825.00**		
Tuition Quarter 1	$6,433.33	Course Materials Fee Quarter 1	$950.00
Tuition Quarter 2	$6,433.34	Course Materials Fee Quarter 2	$950.00
Tuition Quarter 3	$5,958.32	Course Materials Fee Quarter 3	$950.00
Tuition Quarter 4	$4,912.51	Course Materials Fee Quarter 4	$1,000.00
Tuition Quarter 5	$4,437.50	Course Materials Fee Quarter 5	$1,000.00
Tuition Quarter 6	$4,437.50	Course Materials Fee Quarter 6	$1,000.00
Tuition Quarter 7	$4,437.50	Course Materials Fee Quarter 7	$925.00
Total Tuition:	**$37,050.00**	**Total Tuition:**	**$6,775.00**

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

GenEd Course: Introduction to Communication

This course introduces students to the theories and principles of speech communication from a wide range of perspectives. The evolution of communication theory is examined and foundational principles, such as the communication process, perception, verbal and nonverbal communication and listening, are introduced. The dynamics of relationships, intercultural and gender communication issues, and conflict and negotiation are also explored, along with ethical issues inherent in the communication process.

Technical Course: Operating Systems I

- Linked to CompTIA IT Fundamentals and CompTIA A+ certifications
- IT Concepts and Terminology – notational systems, computing basics, and the value of data and troubleshooting
- Infrastructure – Set up and install common peripheral devices to a laptop/PC or secure a basic wireless network
- Applications and Software – various components of an operating system and the purpose of methods of application architecture
- Software Development – programming language categories, logic and the purpose of programming concepts
- Database Fundamentals – database concepts, structure, and purpose, as well as methods used to interface
- Security – confidentiality, integrity and availability concerns of secure devices and best practice methods
- Hardware – Identifying, using and connecting hardware components and devices, including the broad knowledge about different devices that is now necessary to support the remote workforce
- Operating Systems – Install and support Windows OS including command line and client support, system configuration imaging and troubleshooting for Mac OS, Chrome OS, Android and Linux OS
- Software Troubleshooting – Troubleshoot PC and mobile device issues including common OS, malware and security issues
- Networking – Explain types of networks and connections including TCP/IP, WIFI and SOHO
- Troubleshooting – Troubleshoot real-world device and network issues quickly and efficiently
- Security – Identify and protect against security vulnerabilities for devices and their network connections
- Mobile Devices – Install and configure laptops and other mobile devices and support applications to ensure connectivity for end users
- Virtualization and Cloud Computing – Compare and contrast cloud computing concepts and set up client-side virtualization
- Operational Procedures – Follow best practices for safety, environmental impacts, and communication and professionalism

Technical Course: Cloud Security Foundations

- Linked to Microsoft 365 Certified Fundamentals, Microsoft Certified Azure Fundamentals, and (ISC)^2 Certified in Cybersecurity certifications
- Describe cloud concepts
- Describe Microsoft 365 apps and services
- Describe security, compliance, privacy, and trust in Microsoft 365
- Describe Microsoft 365 pricing, licensing, and support
- Describe Azure architecture and services
- Describe Azure management and governance
- Security principles
- Business Continuity (BC), Disaster Recovery (DR), and incident response concepts
- Access control concepts
- Network Security
- Security Operations

GenEd Course: English Composition I

This course helps students develop quality writing skills by explaining and identifying the steps involved in the writing process. The importance of proper grammar, punctuation, and spelling is highlighted, as emphasis is placed on editing and revising pieces of writing. Students also learn proper research techniques, utilizing the Modern Language Association (MLA) style.

Technical Course: Client

- Linked to Microsoft 365 Certified: Endpoint Administrator Associate certification
- Prepare infrastructure for devices
- Add devices to Microsoft Entra ID
- Enroll devices to Microsoft Intune
- Implement identity and compliance
- Manage and maintain devices
- Deploy and upgrade Windows clients by using cloud-based tools
- Plan and implement device configuration profiles
- Implement Intune Suite add-on capabilities

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Client *(continued)*

- Perform remote actions on devices
- Manage applications
- Deploy and update apps
- Plan and implement app protection and app configuration policies
- Protect devices
- Configure endpoint security
- Manage device updates by using Intune

Technical Course: Networking I

Option A

- Linked to Cisco Certified Support Technician (CCST) Networking and Cisco Certified Network Associate (CCNA) certifications
- Explain the role and function of network components
- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- Describe IPv6 address types
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
- Explain virtualization fundamentals (server virtualization, containers, and VRFs)
- Describe switching concepts
- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify interswitch connectivity
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
- Describe Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
- Interpret the components of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2
- Describe the purpose, functions, and concepts of first hop redundancy protocols
- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in a client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features including facilities and levels
- Configure and verify DHCP client and relay
- Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping
- Configure network devices for remote access using SSH
- Describe the capabilities and functions of TFTP/FTP in the network
- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe IPsec remote access and site-to-site VPNs

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Networking I – Option A *(continued)*

- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK
- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture (overlay, underlay, and fabric)
- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data

Option B

- Linked to CompTIA Network+ certification
- Establish network connectivity by deploying wired and wireless devices
- Understand and maintain network documentation
- Understand the purpose of network services
- Understand basic datacenter, cloud and virtual networking concepts
- Monitor network activity, identifying performance and availability issues
- Implement network hardening techniques
- Manage, configure, and troubleshoot network infrastructure

GenEd Course: Critical Thinking and Logic

The aim of this course is to deepen students' skills at everyday logical reasoning and critical thought. The primary learning goals for this course are focused on expanding:

- Understanding the logical structures of the primary classes of arguments used in the everyday contexts of life
- Analyzing arguments within these classes for their strengths and weaknesses
- Recognizing common fallacies in reasoning, including reasoning involving determining probabilities
- Constructing good arguments using principles of informal reasoning
- Reflecting on your own thinking practices
- Listening to the arguments of others without prejudging these arguments in advance

Technical Course: Security I

- Linked to CompTIA Security+ certification
- General Security Concepts – Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls discussed throughout the exam
- Threats, Vulnerabilities, and Mitigations – Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments
- Security Architecture – Includes security implications of different architecture models, principles of securing enterprise infrastructure, and strategies to protect data
- Security Operations – Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software, and data management
- Security Program Management and Oversight – Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness

Technical Course: Networking II

- Linked to Cisco Cybersecurity Associate certification
- Describe the CIA triad
- Compare security deployments
- Describe security terms
- Compare security concepts
- Describe the principles of the defense-in-depth strategy
- Compare access control models

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Networking II *(continued)*

- Describe terms as defined in CVSS
- Identify the challenges of data visibility (network, host, and cloud) in detection
- Identify potential data loss from traffic profiles
- Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- Compare rule-based detection vs. behavioral and statistical detection
- Compare attack surface and vulnerability
- Identify the types of data provided by these technologies
- Describe the impact of these technologies on data visibility
- Describe the uses of these data types in security monitoring
- Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle
- Describe web application attacks, such as SQL injection, command injections, and cross site scripting
- Describe social engineering attacks (manual and generative AI)
- Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
- Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
- Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures, and predictive AI
- Identify components of an operating system (such as Windows and Linux) in a given scenario
- Describe the role of attribution in an investigation
- Identify type of evidence used based on provided logs
- Interpret operating system, SIEM, SOAR platform, application, or command line logs to identify an event
- Interpret the output report of malware analysis tools such as a detonation chamber or sandbox
- Map the provided events to source technologies
- Compare impact and no impact for these items
- Compare deep packet inspection with packet filtering and stateful firewall operation
- Compare inline traffic interrogation and taps or traffic monitoring
- Compare characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in analysis of network traffic
- Extract files from a TCP stream when given a PCAP file and
- Wireshark Identify key elements in an intrusion from a given PCAP file
- Interpret the fields in protocol headers as related to intrusion analysis
- Interpret common artifact elements from an event to identify an alert
- Interpret basic regular expressions
- Describe management concepts
- Describe the elements in an incident response plan as stated in NIST.SP800-61
- Apply the incident handling process such as NIST.SP800-61 to an event
- Map elements to these steps of analysis based on the NIST.SP800-61
- Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800 61)
- Describe concepts as documented in NIST.SP800-86
- Identify these elements used for network profiling
- Identify these elements used for server profiling
- Identify protected data in a network
- Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
- Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

GenEd Course: Communication and Customer Relations

This course introduces students to effective written & verbal communication. They will explore the language of global business, alongside the study of leadership, management and communication across national boundaries with cultural understanding and awareness. In addition, this course provides students with the foundation of sound customer service and customer relations.

Technical Course: Cloud Security I

- Linked to Microsoft Certified Azure Fundamentals, Microsoft Certified Azure Administrator Associate, and Microsoft Certified Information Security Administrator Associate certifications
- Describe cloud concepts

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Cloud Security I *(continued)*

- Describe Azure architecture and services
- Describe Azure management and governance
- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Implement and manage virtual networking
- Monitor and maintain Azure resources
- Implement information protection
- Implement data loss prevention and retention
- Manage risks, alerts, and activities

Technical Course: Networking III

- Linked to Cisco Certified Network Professional (CCNP) Enterprise certification (Part 1)
- Explain the different design principles used in an enterprise network
- Describe wireless network design principles
- Explain the working principles of the Cisco SD-WAN solution
- Explain the working principles of the Cisco SD-Access solution
- Interpret wired and wireless QoS configurations
- Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables
- Describe device virtualization technologies
- Configure and verify data path virtualization technologies
- Describe network virtualization concepts
- Layer 2
- Layer 3
- Wireless
- IP Services

GenEd Course: Employment Preparation

- Job Readiness Workshop
- Entrepreneurship Checklist Session
- Projects include: Disassemble and reassemble PCs and laptops, diagnose and resolve common errors, identify and replace consumable components, soldering, create a cable, assemble a server, troubleshoot hardware and software issues and network connectivity, image a computer, move a user profile from an old computer to a new computer, install a server, install a client OS, configure a computer's static IP address, install and manage active directory, install routers and switches, draw a network diagram, install DHCP and DNS servers, configure a radius server, configure a trust relationship, present a solution for identity management, and present a solution for data loss protection/prevention.

Technical Course: Networking IV

- Linked to Cisco Certified Network Professional (CCNP) Enterprise certification (Part 2)
- Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
- Configure and verify Flexible NetFlow
- Configure SPAN/RSPAN/ERSPAN
- Configure and verify IPSLA
- Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
- Configure and verify NETCONF and RESTCONF
- Configure and verify device access control
- Configure and verify infrastructure security features
- Describe REST API security
- Configure and verify wireless security features

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Networking IV *(continued)*

- Describe the components of network security design
- Interpret basic Python components and scripts
- Construct valid JSON-encoded files
- Describe the high-level principles and benefits of a data modeling language, such as YANG
- Describe APIs for Cisco DNA Center and vManage
- Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
- Construct an EEM applet to automate configuration, troubleshooting, or data collection
- Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

Technical Course: Cloud Security II

- Linked to Amazon AWS Certified Cloud Practitioner and Amazon AWS Certified Solutions Architect – Associate certifications
- Explain the value of the AWS Cloud
- Understand and explain the AWS shared responsibility model
- Understand security best practices
- Understand AWS Cloud costs, economics, and billing practices
- Describe and position the core AWS services, including compute, network, database, and storage services
- Identify AWS services for common use cases
- Design solutions that incorporate AWS services to meet current business requirements and future projected needs
- Design architectures that are secure, resilient, high-performing, and cost optimized
- Review existing solutions and determine improvements

GenEd Course: Group Dynamics

This course focuses on the patterns and dynamics of group interactions, and the communication behavior of individuals within group structures. Topics include a psychosocial approach to group behavior, structure, types, stages, roles, leadership, and facilitation. The class will explore and research decision-making techniques, group problems and problem-solving, resolutions skills, ethics, cultural sensitivity, and the intra-and-inter-personal dynamics within small groups.

Technical Course: Security II

- Linked to Ethical Hacker certification
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

(continued on next page)

Cloud Security *(continued)*

Degree Program

Course Objectives

Technical Course: Security III

- Linked to Microsoft Certified Security, Compliance, and Identity Fundamentals, Systems Security Certified Practitioner (SSCP), and Certified Information Systems Security Professional (CISSP) certifications
- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft Entra
- Describe the capabilities of Microsoft security solutions
- Describe the capabilities of Microsoft compliance solutions
- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Technical Course: Project Management

- Linked to Certified Associate in Project Management (CAPM) and Project Management Professional (PMP) certifications
- Define project management fundamentals
- Define project management within the organization
- Define the project management methodology
- Initiate a project
- Develop a project management plan and plan components
- Plan a project schedule
- Plan project costs
- Plan for quality, resources, and procurements
- Plan for risk
- Plan stakeholder engagement and communications
- Execute a project
- Work with stakeholders
- Monitor project work, scope, risks, stakeholder engagement, and communications
- Control project changes, scope, schedule, costs, quality, resources, and procurements
- Close a project

Technical Course: Cloud Security III

- Linked to Amazon AWS Certified SysOps Administrator – Associate certification
- Support and maintain AWS workloads according to the AWS Well-Architected Framework
- Perform operations by using the AWS Management Console and the AWS CLI
- Implement security controls to meet compliance requirements
- Monitor, log, and troubleshoot systems
- Apply networking concepts (for example, DNS, TCP/IP, firewalls)
- Implement architectural requirements (for example, high availability, performance, capacity)
- Perform business continuity and disaster recovery procedures
- Identify, classify, and remediate incidents

GenEd Course: ITIL Foundation

- Linked to ITIL Foundation certification
- Understand the key concepts of service management
- Understand how the ITIL guiding principles can help an organization adopt and adapt service management
- Understand the four dimensions of service management
- Understand the purpose and components of the ITIL service value system
- Understand the activities of the service value chain, and how they interconnect
- Know the purpose and key terms of 15 ITIL practices
- Understand 7 ITIL practices

VOCATIONAL
CERTIFICATE PROGRAMS

These programs vary in length from one to eight months, and are carefully selected to provide our students with better career opportunities according to industry demand. Vocational programs are designed to train or retrain participants to achieve a meaningful employment outcome such as a new job, a promotion or pay increase, or self-employment in field supported by the completed program of study.

If you have questions about any of these programs, please contact your Career Specialist.

Please note that not all classes may always be available.

Cisco Certified Expert: CCNA

Vocational Program

Program Description

Linked to the Cisco® Certified Network Associate (CCNA®) certification, this program provides students with the essential knowledge to install, configure, and operate simple routed LANs and WANs. The learner will gain knowledge of switched LAN Emulation networks made up of Cisco equipment.

Course Objectives

Course: Cisco Certified Expert: CCNA

- Identify the components of a computer network and describe their basic characteristics; understand host-to-host communication
- Describe the features and functions of the Cisco Internetwork Operating System (IOS®) software
- Describe LANs and the role of switches within LANs
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Install a switch and perform the initial configuration
- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting
- Describe the TCP/IP Transport layer and Application layer
- Explore functions of routing Implement basic configuration on a Cisco router
- Explain host-to-host communications across switches and routers
- Identify and resolve common switched network issues and common problems associated with IPv4 addressing
- Describe IPv6 main features and addresses, and configure and verify basic IPv6 connectivity
- Describe the operation, benefits, and limitations of static routing
- Describe, implement, and verify Virtual Local Area Networks (VLANs) and trunks
- Describe the application and configuration of inter-VLAN routing
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF)
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work
- Configure link aggregation using EtherChannel
- Describe the purpose of Layer 3 redundancy protocols; Describe basic WAN and VPN concepts
- Describe the operation of Access Control Lists (ACLs) and their applications in the network
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients; configure Network Address Translation (NAT) on Cisco routers
- Describe basic Quality of Service (QoS) concepts
- Describe concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs)
- Describe network and device architectures and introduce virtualization
- Introduce the concept of network programmability and Software-Defined Networking (SDN) and describe smart network management solutions such as Cisco DNA Center™, Software-Defined Access (SD-Access), and Software-Defined Wide Area Network (SD-WAN)
- Configure basic IOS system monitoring tools
- Describe the management of Cisco devices, the current security threat landscape, and threat defense technologies
- Implement a basic security configuration of the device management plane; Implement basic steps to harden network devices

Job Titles That Correlate to This Program

Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	Networking experience recommended
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Cloud Security Certified Professional: Azure and AWS

Vocational Program

Program Description
The Cloud Security Certified Professional: Azure and AWS program is designed to prepare students to implement, monitor, and maintain Microsoft Azure solutions, including major services related to compute, storage, network, and security. Students will also learn to conduct big data analysis with practical, real-world examples; covering the fundamentals of building IT infrastructure on Amazon Web Services (AWS), and optimizing the use of AWS Cloud by understanding AWS services and how they fit into cloud-based solutions. Completers will be prepared to pursue DevOps, support, and cloud operations roles.

Courses include preparation for industry standard certifications AWS Certified Cloud Practitioner, AWS Certified Solutions Architect – Associate, Microsoft Certified Azure Fundamentals, Microsoft Certified Azure Administrator Associate, AWS Certified SysOps Administrator – Associate, AWS Certified Developer – Associate, Microsoft Certified Azure Security Engineer Associate, Microsoft Certified Azure Developer Associate, Microsoft Certified Azure Solutions Architect Expert, Microsoft Certified Azure Database Administrator Associate, and AWS Certified Data Analytics – Specialty.

This program is 600 total contact hours over 25-30 weeks. Classes are typically offered in the daytime Monday through Thursday from 9:30am until 2:30pm; or in the evening Monday through Thursday from 5:30pm until 10:30pm. In order to complete the Cloud Security Certified Professional: Azure and AWS program, students must complete all six of the courses listed below:

	Contact (Clock) Hours		
Required Courses	**Lecture**	**Lab**	**Total Hours**
Cloud I	40	60	100
Cloud II	40	60	100
Cloud Security I	40	60	100
Cloud Security II	40	60	100
Cloud Data I	40	60	100
Cloud Data II	40	60	100
Total:	**240**	**360**	**600**

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program
Information Security Analyst, Information Security Administrator, Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	600 Clock Hours (7.5 Months)
Lecture/Lab Hours:	240/360
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$18,750.00**
Course Materials Fee (nonrefundable):	**$2,850.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	***Tuition***	***Course Materials***	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Cloud I	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud II	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Security I	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Security II	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Data I	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Data II	***$3,125.00***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
TOTAL:	***$18,750.00***	***$2,850.00***				

(continued on next page)

Cloud Security Certified Professional: Azure and AWS *(continued)*

Vocational Program

Course Objectives

Course: Cloud I

- Describe how cloud adoption transforms the way IT systems work and the benefits of cloud computing with AWS
- Discuss how to design systems that are secure, reliable, high performing, and cost efficient
- Describe principles to consider when migrating or designing new applications for the cloud
- Identify the design patterns and architectural options applied in a variety of use cases
- Define high availability, fault tolerance, and scalability, and discuss how to avoid single points of failure
- List AWS services that have built-in fault tolerance or can be designed for fault tolerance
- Describe why load balancing is key architectural component for AWS-powered applications
- Identify the benefits of Infrastructure as Code
- Describe how to leverage the capabilities of AWS to support automation
- Create, manage, provision, and update related resources using AWS CloudFormation
- Articulate the importance of making systems highly cohesive and loosely coupled
- Describe system coupling to support the distributed nature of applications built for the cloud
- Describe database services for storing and deploying web-accessible
- Compare structured query language—or SQL—databases with NoSQL databases
- Describe how the AWS Well-Architected Framework improves cloud-based architectures
- Describe the business impact of design decisions
- Identify the design principles and best practices of the Operational Excellence pillar
- Describe how to secure data at every layer in the application
- Describe the appropriate tools and services to provide security focused content
- Describe the design principles and the best practices of the Reliability pillar
- Select compute, storage, database, and networking resources to improve performance
- Evaluate the most important performance metrics for your applications; eliminate unneeded costs or suboptimal resources
- Troubleshoot common errors

Course: Cloud II

- Manage workflow
- Install and configure desktop operating systems and applications
- Troubleshoot the desktop operating system, desktop applications, and desktop networking and connectivity
- Install and configure hardware devices and drivers (including mobile and personal devices)
- Troubleshoot hardware devices and drivers (including mobile and personal devices)
- Escalate complex issues to the appropriate administrator (for example, server administrator, network administrator, or desktop configuration administrator)
- Install and test department-specific and line-of-business (LOB) applications on end-user computers
- Change desktop configurations as needed
- Re-image desktops as needed

Course: Cloud Security I

- Understand AWS infrastructure as it relates to system operations, such as global infrastructure, core services, and account security
- Use the AWS Command Line Interface (AWS CLI), and understand additional administration and development tools
- Manage, secure, and scale compute instances on AWS
- Manage, secure, and scale configurations
- Identify container services and AWS services that are available for serverless computing
- Manage, secure, and scale databases on AWS
- Build virtual private networks with Amazon Virtual Private Cloud (Amazon VPC)
- Configure and manage storage options using the storage services offered with AWS
- Monitor the health of your infrastructure with services such as Amazon CloudWatch, AWS CloudTrail, and AWS Config
- Manage resource consumption in an AWS account by using tags, Amazon CloudWatch, and AWS Trusted Advisor
- Create and configure automated and repeatable deployments with tools such as Amazon Machine Images (AMIs) and AWS CloudFormation
- Develop and run a simple program in AWS Cloud9
- Understand AWS Identity and Access Management
- Develop storage solutions with Amazon S3
- Develop flexible NoSQL solutions with Amazon DynamoDB
- Develop and deploy secure applications on AWS

(continued on next page)

Cloud Security Certified Professional: Azure and AWS *(continued)*

Vocational Program

Course Objectives

Course: Cloud Security II

- Manage identity and access
- Implement platform protection
- Manage security operations
- Secure data and applications
- Implement IaaS solutions and Azure functions
- Create Azure App Service Web Apps
- Develop for Azure storage using Cosmos DB storage and blob storage
- Implement Azure security with user authentication, authorization, and secure cloud solutions
- Monitor, troubleshoot, and optimize Azure solutions
- Implement API management
- Develop event-based and message-based solutions

Course: Cloud Data I

- Configure Azure Active Directory for workloads
- Configure Azure AD Privileged Identity Management
- Configure Azure tenant security
- Implement platform protection, including implementing network security, host security, container security, and Azure Resource Management security
- Manage security operations, including security services, policies, and alerts
- Configure security policies to manage data, and secure data infrastructure
- Configure encryption for data at rest
- Configure and manage Key Vault

Course: Cloud Data II

- Plan and implement data platform resources
- Implement a secure environment
- Monitor and optimize operational resources
- Optimize query performance
- Perform automation of tasks
- Plan and implement a High Availability and Disaster Recovery (HADR) environment
- Perform administration by using T-SQL

CompTIA Certified Expert: Network+

Vocational Program

Program Description

Participants who complete the CompTIA Certified Expert: Network+ program will acquire the skills needed to develop a career in IT infrastructure, covering troubleshooting, configuring, and managing both wired and wireless networks. Students will also learn critical security concepts; key cloud computing best practices and typical service models; and updated hardware and virtualization techniques and concepts. This course includes preparation for the CompTIA Network+ certification.

Course Objectives

Course: CompTIA Certified Expert: Network+

- Basic components and characteristics of a network
- Host-to-network and network-to-network connections
- LAN wiring components and conventions
- Differentiate between wired networking devices
- How to configure your workstation, switch, and router
- TCP/IP communications protocols basics
- Practical overview of IP subnetting and how it works
- Wireless networking components
- Common security threats and mitigation techniques
- Securing systems and network devices
- Controlling access to the network
- Monitoring network resources
- Troubleshooting the network

Job Titles That Correlate to This Program

Systems Administrator, Network Administrator, Network Engineer, Information Technology Specialist (IT Specialist), Local Area Network Administrator (LAN Administrator), Information Technology Manager (IT Manager), Information Technology Director (IT Director), Systems Engineer, Network Manager, Network Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	Some networking experience recommended
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

CompTIA Certified Expert: Security+

Vocational Program

Program Description

The CompTIA Certified Expert: Security+ program establishes the core knowledge required in any cybersecurity role. Program completers will learn to assess the security posture of an enterprise environment; recommend and implement appropriate security solutions; monitor and secure hybrid environments; operate with an awareness of applicable laws and policies; and identify, analyze, and respond to security events and incidents. This course includes preparation for the CompTIA Security+ certification.

Course Objectives

Course: CompTIA Certified Expert: Security+

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions
- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Job Titles That Correlate to This Program

Information Security Analyst, Information Security Administrator, or other similar jobs, Network Administrator, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	At least 2 years of experience in IT Administration with a security focus
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cybersecurity Certified Associate

Vocational Program

Program Description

The Cybersecurity Certified Associate program is designed to help students gain the knowledge and skills necessary to be confident and ready to work in the Information Technology field. Completers will be prepared to work in a variety of positions including Help Desk Support, IT Support Specialist, Network Technician, Information Security Analyst, Network Administrator, Computer Network Architect, Computer Systems Analyst, or other similar jobs.

Students will gain security and risk management skills that are among the most highly sought-after skills in networking. Additionally, completers will have hands-on knowledge of server configuration, client connectivity, security, networking, Active Directory, DNS, DHCP, troubleshooting, optimization and backup/recovery of critical data.

Courses include preparation for industry standard certifications CompTIA IT Fundamentals, CompTIA A+, Microsoft 365 Certified Fundamentals, Microsoft Certified Azure Fundamentals, (ISC)2 Certified in Cybersecurity, Microsoft 365 Certified Endpoint Administrator Associate, Cisco Certified Support Technician (CCST) Networking, Cisco Certified Network Associate (CCNA), CompTIA Network+, Microsoft Certified: Security, Compliance, and Identity Fundamentals, CompTIA Security+, and Cisco Cybersecurity Associate.

This program is 600 total contact hours over a 25-30 week period. Classes are typically offered in the daytime Monday through Thursday from 9:30am until 2:30pm; or in the evening from 5:30pm until 10:30pm. In order to complete the Cybersecurity Certified Associate program, students must complete all seven of the courses listed below:

	Contact (Clock) Hours		
Required Courses	**Lecture**	**Lab**	**Total Hours**
Operating Systems I	40	60	100
Cloud Security Fundamentals	40	60	100
Client	40	60	100
Networking I	40	60	100
Security I	40	60	100
Networking II	40	60	100
Total:	**240**	**360**	**600**

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	600 Clock Hours (7.5 Months)
Lecture/Lab Hours:	240/360
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Tuition for Program:	**$19,300.00**
Course Materials Fee (nonrefundable):	**$2,850.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	***Tuition***	***Course Materials***	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Operating Systems I	***$3,216.67***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Cloud Security Fundamentals	***$3,216.67***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Client	***$3,216.67***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Networking I	***$3,216.67***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Security I	***$3,216.66***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
Networking II	***$3,216.66***	***$475.00***	*$150.00*	*$200.00*	*$100.00*	*$25.00*
TOTAL:	***$19,300.00***	***$2,850.00***				

(continued on next page)

Cybersecurity Certified Associate *(continued)*

Vocational Program

Course Objectives

Course: Operating Systems I

- Linked to CompTIA IT Fundamentals and CompTIA A+ certifications
- IT Concepts and Terminology – notational systems, computing basics, and the value of data and troubleshooting
- Infrastructure – Set up and install common peripheral devices to a laptop/PC or secure a basic wireless network
- Applications and Software – various components of an operating system and the purpose of methods of application architecture
- Software Development – programming language categories, logic and the purpose of programming concepts
- Database Fundamentals – database concepts, structure, and purpose, as well as methods used to interface
- Security – confidentiality, integrity and availability concerns of secure devices and best practice methods
- Hardware – Identifying, using and connecting hardware components and devices, including the broad knowledge about different devices that is now necessary to support the remote workforce
- Operating Systems – Install and support Windows OS including command line and client support, system configuration imaging and troubleshooting for Mac OS, Chrome OS, Android and Linux OS
- Software Troubleshooting – Troubleshoot PC and mobile device issues including common OS, malware and security issues
- Networking – Explain types of networks and connections including TCP/IP, WIFI and SOHO
- Troubleshooting – Troubleshoot real-world device and network issues quickly and efficiently
- Security – Identify and protect against security vulnerabilities for devices and their network connections
- Mobile Devices – Install and configure laptops and other mobile devices and support applications to ensure connectivity for end users
- Virtualization and Cloud Computing – Compare and contrast cloud computing concepts and set up client-side virtualization
- Operational Procedures – Follow best practices for safety, environmental impacts, and communication and professionalism

Course: Cloud Security Foundations

- Linked to Microsoft 365 Certified Fundamentals, Microsoft Certified Azure Fundamentals, and (ISC)^2 Certified in Cybersecurity certifications
- Describe cloud concepts
- Describe Microsoft 365 apps and services
- Describe security, compliance, privacy, and trust in Microsoft 365
- Describe Microsoft 365 pricing, licensing, and support
- Describe Azure architecture and services
- Describe Azure management and governance
- Security principles
- Business Continuity (BC), Disaster Recovery (DR), and incident response concepts
- Access control concepts
- Network Security
- Security Operations

Course: Client

- Linked to Microsoft 365 Certified: Endpoint Administrator Associate certification
- Prepare infrastructure for devices
- Add devices to Microsoft Entra ID
- Enroll devices to Microsoft Intune
- Implement identity and compliance
- Manage and maintain devices
- Deploy and upgrade Windows clients by using cloud-based tools
- Plan and implement device configuration profiles
- Implement Intune Suite add-on capabilities
- Perform remote actions on devices
- Manage applications
- Deploy and update apps
- Plan and implement app protection and app configuration policies
- Protect devices
- Configure endpoint security
- Manage device updates by using Intune

(continued on next page)

Cybersecurity Certified Associate *(continued)*

Vocational Program

Course Objectives

Course: Networking I

Option A

- Linked to Cisco Certified Support Technician (CCST) Networking and Cisco Certified Network Associate (CCNA) certifications
- Explain the role and function of network components
- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- Describe IPv6 address types
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
- Explain virtualization fundamentals (server virtualization, containers, and VRFs)
- Describe switching concepts
- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify interswitch connectivity
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
- Describe Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
- Interpret the components of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2
- Describe the purpose, functions, and concepts of first hop redundancy protocols
- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in a client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features including facilities and levels
- Configure and verify DHCP client and relay
- Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping
- Configure network devices for remote access using SSH
- Describe the capabilities and functions of TFTP/FTP in the network
- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe IPsec remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK
- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture (overlay, underlay, and fabric)
- Explain AI (generative and predictive) and machine learning in network operations

(continued on next page)

Cybersecurity Certified Associate *(continued)*

Vocational Program

Course Objectives

Course: Networking I – Option A *(continued)*

- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data

Option B

- Linked to CompTIA Network+ certification
- Establish network connectivity by deploying wired and wireless devices
- Understand and maintain network documentation
- Understand the purpose of network services
- Understand basic datacenter, cloud and virtual networking concepts
- Monitor network activity, identifying performance and availability issues
- Implement network hardening techniques
- Manage, configure, and troubleshoot network infrastructure

Course: Security I

- Linked to CompTIA Security+ certification
- General Security Concepts – Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls discussed throughout the exam
- Threats, Vulnerabilities, and Mitigations – Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments
- Security Architecture – Includes security implications of different architecture models, principles of securing enterprise infrastructure, and strategies to protect data
- Security Operations – Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software, and data management
- Security Program Management and Oversight – Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness

Course: Networking II

- Linked to Cisco Cybersecurity Associate certification
- Describe the CIA triad
- Compare security deployments
- Describe security terms
- Compare security concepts
- Describe the principles of the defense-in-depth strategy
- Compare access control models
- Describe terms as defined in CVSS
- Identify the challenges of data visibility (network, host, and cloud) in detection
- Identify potential data loss from traffic profiles
- Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- Compare rule-based detection vs. behavioral and statistical detection
- Compare attack surface and vulnerability
- Identify the types of data provided by these technologies
- Describe the impact of these technologies on data visibility
- Describe the uses of these data types in security monitoring
- Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle
- Describe web application attacks, such as SQL injection, command injections, and cross site scripting
- Describe social engineering attacks (manual and generative AI)
- Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
- Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
- Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures, and predictive AI
- Identify components of an operating system (such as Windows and Linux) in a given scenario
- Describe the role of attribution in an investigation

(continued on next page)

Cybersecurity Certified Associate *(continued)*

Vocational Program

Course Objectives

Course: Networking II *(continued)*

- Identify type of evidence used based on provided logs
- Interpret operating system, SIEM, SOAR platform, application, or command line logs to identify an event
- Interpret the output report of malware analysis tools such as a detonation chamber or sandbox
- Map the provided events to source technologies
- Compare impact and no impact for these items
- Compare deep packet inspection with packet filtering and stateful firewall operation
- Compare inline traffic interrogation and taps or traffic monitoring
- Compare characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in analysis of network traffic
- Extract files from a TCP stream when given a PCAP file and
- Wireshark Identify key elements in an intrusion from a given PCAP file
- Interpret the fields in protocol headers as related to intrusion analysis
- Interpret common artifact elements from an event to identify an alert
- Interpret basic regular expressions
- Describe management concepts
- Describe the elements in an incident response plan as stated in NIST.SP800-61
- Apply the incident handling process such as NIST.SP800-61 to an event
- Map elements to these steps of analysis based on the NIST.SP800-61
- Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800 61)
- Describe concepts as documented in NIST.SP800-86
- Identify these elements used for network profiling
- Identify these elements used for server profiling
- Identify protected data in a network
- Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
- Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

Cybersecurity Certified Manager

Vocational Program

Program Description

The goal of this program is to prepare students to work in the Information Technology field in a variety of positions working with Desktops, Servers, Networks, and more. Courses include preparation for industry standard certification in Microsoft 365 Certified Enterprise Administrator Expert, Microsoft Certified Azure Solutions Architect Expert, Certified Ethical Hacker (CEH), Cisco Certified Networking Professional (CCNP), Certified Associate in Project Management (CAPM), Project Management Professional (PMP), Certified Information Security Manager (CISM), and Information Technology Infrastructure Library (ITIL) Foundation.

This program is 600 total contact hours over a 25-30 week period. Classes are typically offered in the daytime Monday through Thursday from 9:30am until 2:30pm; or in the evening from 5:30pm until 10:30pm. In order to complete the Cybersecurity Certified Manager program, students must complete all seven of the courses listed below:

	Contact (Clock) Hours		
Required Courses	**Lecture**	**Lab**	**Total Hours**
Networking and Security VII	40	60	100
Networking and Security VIII	40	60	100
Networking and Security IX	40	60	100
Networking and Security X	40	60	100
Networking and Security XI	40	60	100
Networking and Security XII	40	60	100
Total:	**240**	**360**	**600**

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	600 Clock Hours (7.5 Months)
Lecture/Lab Hours:	240/360
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	Previous experience in IT, networking, server administration recommended
Tuition for Program:	**$18,700.00**
Course Materials Fee (nonrefundable):	**$3,000.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	***Tuition***	***Course Materials***	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Networking and Security VII	***$3,116.67***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security VIII	***$3,116.67***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security IX	***$3,116.67***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security X	***$3,116.67***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security XI	***$3,116.66***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security XII	***$3,116.66***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
TOTAL:	***$18,700.00***	***$3,000.00***				

(continued on next page)

Cybersecurity Certified Manager *(continued)*

Vocational Program

Course Objectives

Course: Networking and Security VII

- Design and implement Microsoft 365 services
- Manage user identity and roles; access and authentication
- Plan Office 365 workloads and applications
- Implement modern device services, Microsoft 365 security, and threat management
- Manage Microsoft 365 governance and compliance

Course: Networking and Security VIII

- Implement and monitor an Azure infrastructure; management and security solutions; solutions for apps; and data platforms
- Design monitoring, identity and security, data storage, business community, and infrastructure
- Understand how perimeter defenses work, and how intruders escalate privileges

Course: Networking and Security IX

- Secure various systems against intrusion
- Understanding Intrusion Detection, Policy Creation, Social Engineering, DDos Attacks, Buffer Overflows, and Virus Creation
- Implement and optimize Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6

Course: Networking and Security X

- Implement External Border Gateway Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking
- Implement network redundancy using protocols (incl. Hot Standby Routing Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP))
- Implement internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT)
- Implement overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP)
- Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager

Course: Networking and Security XI

- Understand service management as a practice; and the ITIL service lifecycle
- Understand generic concepts and definitions of the ITIL service lifecycle; key principles and models; selected processes, functions, and roles; technology and architecture; competence and training
- Define and develop a project management plan and plan components
- Plan a project schedule, project costs; Plan for quality, resources, procurements, and risk
- Initiate and execute a project
- Monitor project work, scope, risks, stakeholder engagement, and communications
- Control project changes, scope, schedule, costs, quality, resources, and procurements

Course: Networking and Security XII

- Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations
- Identify and manage information security risks to achieve business objectives
- Create a program to implement the information security strategy
- Implement an information security program
- Oversee and direct information security activities to execute the information security program
- Plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents

Cybersecurity Certified Professional

Vocational Program

Program Description
The Cybersecurity Certified Professional program is designed to help students gain the knowledge and skills necessary to be confident and ready to work in the Information Technology field at the professional level. Completers will be prepared to work in a variety of positions including Help Desk Support, IT Support Specialist, Network Technician, Information Security Analyst, Network Administrator, Computer Network Architect, Computer Systems Analyst, or other similar jobs.

Students will gain security and risk management skills that are among the most highly sought-after skills in networking. Additionally, completers will have hands-on knowledge of server configuration, client connectivity, security, networking, Active Directory, DNS, DHCP, troubleshooting, optimization and backup/recovery of critical data.

Courses include preparation for industry standard certifications Microsoft Certified Azure Fundamentals, Microsoft Certified Azure Administrator Associate, Microsoft Certified Information Security Administrator Associate, Cisco Certified Support Technician (CCST) Networking, Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP) Enterprise, Amazon AWS Certified Cloud Practitioner, Amazon AWS Certified Solutions Architect – Associate, Ethical Hacker, Microsoft Certified Security, Compliance, and Identify Fundamentals, Systems Security Certified Professional (SSCP), and Certified Information Systems Security Professional (CISSP). Classes meet in state-of-the-art computer labs that offer the latest in networking technology.

This program is 600 total contact hours over a 25-30 week period. Classes are typically offered in the daytime Monday through Thursday from 9:30am until 2:30pm; or in the evening from 5:30pm until 10:30pm. In order to complete the Cybersecurity Certified Professional program, students must complete all seven of the courses listed below:

	Contact (Clock) Hours		
Required Courses	**Lecture**	**Lab**	**Total Hours**
Cloud Security I	40	60	100
Networking III	40	60	100
Networking IV	40	60	100
Cloud Security II	40	60	100
Security II	40	60	100
Security III	40	60	100
Total:	**240**	**360**	**600**

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program
Information Security Analyst, Information Security Administrator, Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	600 Clock Hours (7.5 Months)
Lecture/Lab Hours:	240/360
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$18,750.00**
Course Materials Fee (nonrefundable):	**$3,000.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	***Tuition***	***Course Materials***	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Server I	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security II	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security III	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security IV	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security V	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
Networking and Security VI	***$3,125.00***	***$500.00***	*$150.00*	*$225.00*	*$100.00*	*$25.00*
TOTAL:	***$18,750.00***	***$3,000.00***				

(continued on next page)

Cybersecurity Certified Professional *(continued)*

Vocational Program

Course Objectives

Course: Cloud Security I

- Linked to Microsoft Certified Azure Fundamentals, Microsoft Certified Azure Administrator Associate, and Microsoft Certified Information Security Administrator Associate certifications
- Describe cloud concepts
- Describe Azure architecture and services
- Describe Azure management and governance
- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Implement and manage virtual networking
- Monitor and maintain Azure resources
- Implement information protection
- Implement data loss prevention and retention
- Manage risks, alerts, and activities

Course: Networking III

Option A

- Linked to Cisco Certified Support Technician (CCST) Networking and Cisco Certified Network Associate (CCNA) certifications
- Explain the role and function of network components
- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting
- Describe private IPv4 addressing
- Configure and verify IPv6 addressing and prefix
- Describe IPv6 address types
- Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- Describe wireless principles
- Explain virtualization fundamentals (server virtualization, containers, and VRFs)
- Describe switching concepts
- Configure and verify VLANs (normal range) spanning multiple switches
- Configure and verify interswitch connectivity
- Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
- Describe Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
- Interpret the components of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2
- Describe the purpose, functions, and concepts of first hop redundancy protocols
- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in a client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features including facilities and levels
- Configure and verify DHCP client and relay

(continued on next page)

Cybersecurity Certified Professional *(continued)*

Vocational Program

Course Objectives

Course: Networking III – Option A *(continued)*

- Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping
- Configure network devices for remote access using SSH
- Describe the capabilities and functions of TFTP/FTP in the network
- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe IPsec remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK
- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture (overlay, underlay, and fabric)
- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data

Option B

- Linked to Cisco Certified Network Professional (CCNP) Enterprise certification (Part 1)
- Explain the different design principles used in an enterprise network
- Describe wireless network design principles
- Explain the working principles of the Cisco SD-WAN solution
- Explain the working principles of the Cisco SD-Access solution
- Interpret wired and wireless QoS configurations
- Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables
- Describe device virtualization technologies
- Configure and verify data path virtualization technologies
- Describe network virtualization concepts
- Layer 2
- Layer 3
- Wireless
- IP Services

Course: Networking IV

Option A

- Linked to Cisco Cybersecurity Associate certification
- Describe the CIA triad
- Compare security deployments
- Describe security terms
- Compare security concepts
- Describe the principles of the defense-in-depth strategy
- Compare access control models
- Describe terms as defined in CVSS
- Identify the challenges of data visibility (network, host, and cloud) in detection
- Identify potential data loss from traffic profiles
- Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- Compare rule-based detection vs. behavioral and statistical detection
- Compare attack surface and vulnerability

(continued on next page)

Cybersecurity Certified Professional *(continued)*

Vocational Program

Course Objectives

Course: Networking IV – Option A *(continued)*

- Identify the types of data provided by these technologies
- Describe the impact of these technologies on data visibility
- Describe the uses of these data types in security monitoring
- Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle
- Describe web application attacks, such as SQL injection, command injections, and cross site scripting
- Describe social engineering attacks (manual and generative AI)
- Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
- Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
- Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures, and predictive AI
- Identify components of an operating system (such as Windows and Linux) in a given scenario
- Describe the role of attribution in an investigation
- Identify type of evidence used based on provided logs
- Interpret operating system, SIEM, SOAR platform, application, or command line logs to identify an event
- Interpret the output report of malware analysis tools such as a detonation chamber or sandbox
- Map the provided events to source technologies
- Compare impact and no impact for these items
- Compare deep packet inspection with packet filtering and stateful firewall operation
- Compare inline traffic interrogation and taps or traffic monitoring
- Compare characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in analysis of network traffic
- Extract files from a TCP stream when given a PCAP file and
- Wireshark Identify key elements in an intrusion from a given PCAP file
- Interpret the fields in protocol headers as related to intrusion analysis
- Interpret common artifact elements from an event to identify an alert
- Interpret basic regular expressions
- Describe management concepts
- Describe the elements in an incident response plan as stated in NIST.SP800-61
- Apply the incident handling process such as NIST.SP800-61 to an event
- Map elements to these steps of analysis based on the NIST.SP800-61
- Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800 61)
- Describe concepts as documented in NIST.SP800-86
- Identify these elements used for network profiling
- Identify these elements used for server profiling
- Identify protected data in a network
- Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
- Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

Option B

- Linked to Cisco Certified Network Professional (CCNP) Enterprise certification (Part 2)
- Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog
- Configure and verify Flexible NetFlow
- Configure SPAN/RSPAN/ERSPAN
- Configure and verify IPSLA
- Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
- Configure and verify NETCONF and RESTCONF
- Configure and verify device access control
- Configure and verify infrastructure security features
- Describe REST API security
- Configure and verify wireless security features
- Describe the components of network security design

(continued on next page)

Cybersecurity Certified Professional *(continued)*

Vocational Program

Course Objectives

Course: Networking IV – Option B *(continued)*

- Interpret basic Python components and scripts
- Construct valid JSON-encoded files
- Describe the high-level principles and benefits of a data modeling language, such as YANG
- Describe APIs for Cisco DNA Center and vManage
- Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
- Construct an EEM applet to automate configuration, troubleshooting, or data collection
- Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

Course: Cloud Security II

- Linked to Amazon AWS Certified Cloud Practitioner and Amazon AWS Certified Solutions Architect – Associate certifications
- Explain the value of the AWS Cloud
- Understand and explain the AWS shared responsibility model
- Understand security best practices
- Understand AWS Cloud costs, economics, and billing practices
- Describe and position the core AWS services, including compute, network, database, and storage services
- Identify AWS services for common use cases
- Design solutions that incorporate AWS services to meet current business requirements and future projected needs
- Design architectures that are secure, resilient, high-performing, and cost optimized
- Review existing solutions and determine improvements

Course: Security II

- Linked to Ethical Hacker certification
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

Course: Security III

- Linked to Microsoft Certified Security, Compliance, and Identity Fundamentals, Systems Security Certified Practitioner (SSCP), and Certified Information Systems Security Professional (CISSP) certifications
- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft Entra
- Describe the capabilities of Microsoft security solutions
- Describe the capabilities of Microsoft compliance solutions

(continued on next page)

Cybersecurity Certified Professional *(continued)*

Vocational Program

Course Objectives

Course: Security III *(continued)*

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Data Science Architect Boot Camp

Vocational Program

Program Description
The goal of this program is for students to gain proficiency in Data Science; preparing them to work on real-world projects in R, Apache Spark, Scala, Deep Learning, Tableau, Data Science with SAS, SQL, MongoDB, and more.

The Data Science Architect Boot Camp program has been designed keeping in mind the needs of the industry when it comes to the domain of Data Science. Today's Data Scientists need to have a diverse set of skills, including working with huge volumes of data, parsing that data, converting it into a format that is easily understandable, and deriving business insights.

Completers will be prepared to work in a variety of positions in the Data Science field, and to obtain at least one of the following certifications:

- Spark component of Cloudera Spark and Hadoop Developer Certification (CCA175)
- Tableau Desktop Qualified Associate Exam
- SAS Certified Base Programmer Exam
- C100DEV: MongoDB Certified Developer Associate Exam
- Microsoft 70-761 SQL Server Certification Exam
- Microsoft 70-762 SQL Server Certification Exam

This program is 600 total contact hours over a 25-30 week period. Classes are typically offered in the daytime Monday through Thursday from 9:00am until 3:00pm; or in the evening Monday through Thursday from 4:30pm until 10:30pm. In order to complete the Data Science Architect Boot Camp program, students must complete all seven of the courses listed below:

	Contact (Clock) Hours		
Required Courses	**Lecture**	**Lab**	**Total Hours**
Data Science with R	36	54	90
Python for Data Science	36	54	90
Machine Learning	36	54	90
Artificial Intelligence and Deep Learning with Tensorflow	36	54	90
Big Data Hadoop and Spark	36	54	90
Tableau Desktop	30	45	75
Data Science with SAS	30	45	75
Total:	**240**	**360**	**600**

Course Objectives are listed beginning on the next page.

Job Titles That Correlate to This Program
Database Administrator, Software Developer, Computer Programmer, Computer and Information Research Scientist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	600 Clock Hours (25 Weeks)
Lecture/Lab Hours:	240/360
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$16,500.00**
Course Materials Fee (nonrefundable):	**$2,275.00**

Tuition and Fees Breakdown by Course:

			Included in Course Materials Fee (nonrefundable)			
Course Name	*Tuition*	*Course Materials*	*Digital Course Content*	*Virtual Labs*	*Practice Tests*	*eBooks*
Data Science with R	***$2,357.14***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Python for Data Science	***$2,357.14***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Machine Learning	***$2,357.14***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Artificial Intelligence and Deep Learning with Tensorflow	***$2,357.14***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Big Data Hadoop and Spark	***$2,357.14***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Tableau Desktop	***$2,357.15***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
Data Science with SAS	***$2,357.15***	***$325.00***	*$150.00*	*$150.00*	*$0.00*	*$25.00*
TOTAL:	***$18,750.00***	***$2,275.00***				

(continued on next page)

Data Science Architect Boot Camp *(continued)*

Vocational Program

Course Objectives

Course: Data Science with R

- Data Exploration
- Data Manipulation
- Data Visualization
- Introduction to Statistics
- Machine Learning
- Logistic Regression
- Decision Trees and Random Forest
- Unsupervised Learning
- Association Rule Mining and Recommendation Engine
- Introduction to Artificial Intelligence
- Time Series Analysis
- Support Vendor Machine (SVM)
- Naïve Bayes
- Text Mining

Course: Python for Data Science

- Python Environment Setup and Essentials
- Python Language Basic Constructs
- OOP Concepts in Python and Database Connection
- NumPy for Mathematical Computing
- SciPy for Scientific Computing
- Matplotlib for Data Visualization
- Pandas for Data Analysis and Machine Learning
- Scikit-Learn for Natural Language Processing
- Web Scrapping with Python
- Python Deployed for Hadoop
- Python for Apache Spark Coding

Course: Machine Learning

- Supervised Learning and Linear Regression
- Classification and Logistic Regression
- Decision Tree and Random Forest
- Naïve Bayes and Support Vector Machine
- Unsupervised Learning
- Natural language Processing and Text Mining
- Introduction to Deep Learning
- Time Series Analysis

Course: Artificial Intelligence and Deep Learning with Tensorflow

- Multi-Layered Neural Networks
- Training of Neural Networks
- Deep Learning Libraries
- Keras API
- TFLearn API for TensorFLow
- DNN: Deep Neural Networks
- CNN: Convolutional Neural Networks
- RNN: Recurrent Neural Networks
- GPU in Deep Learning
- Autoencoders and Restricted Boltzmann Matching (RBM)
- Deep Learning Applications
- Chatbots

Course: Big Data Hadoop and Spark

- Hadoop Installation and Setup
- Introduction to Big Data Hadoop and Understanding HDFS and MapReduce

(continued on next page)

Data Science Architect Boot Camp *(continued)*

Vocational Program

Course Objectives

Course: Big Data Hadoop and Spark *(continued)*

- Deep Dive in MapReduce
- Introduction to Hive
- Advanced Hive and Impala
- Introduction to Pig
- Flume, Sqoop and HBase
- Writing Spark Applications Using Scala
- Spark Framework
- RDD in Spark
- Data Frames and Spark SQL
- Machine Learning Using Spark (MLlib)
- Integrating Apache Flume and Apache Kafka
- Spark Streaming
- Hadoop Administration – Multi-node Cluster Setup Using Amazon EC2

Course: Tableau Desktop

- Introduction to Data Visualization and Power of Tableau
- Architecture of Tableau
- Working with Metadata and Data Blending
- Creation of Sets
- Working with Filters
- Organizing Data and Visual Analytics
- Working with Mapping
- Working with Calculations and Expressions
- Working with Parameters
- Charts and Graphs
- Dashboards and Stories
- TableauPrep
- Integration of Tableau with R and Hadoop

Course: Data Science with SAS

- Introduction to SAS
- SAS Enterprise Guide
- SAS Operators and Functions
- Compilation and Execution
- Using Variables
- Creation and Compilation of SAS Data Sets
- SAS Procedures
- Input Statement and Formatted Input
- SAS Format
- SAS Graphs
- Interactive Data Processing
- Data Transformation Function
- Output Delivery System (ODS)
- SAS MACROS
- PROC SQL Advanced Base SAS
- Summarization Reports

Microsoft Certified Expert:

Microsoft 365 Certified Modern Desktop Administrator Associate

Vocational Program

Program Description

The Microsoft Certified Expert Microsoft 365 Certified Modern Desktop Administrator Associate program will prepare students to deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment.

Students will learn to configure domain name system (DNS) for active directory, including DNS server settings, zone transfers and replication, active directory infrastructure, trusts, sites, and management services. They will create, maintain, and assess active directory objects – accounts, group policies, software, backup and recovery, file servers, network security/access, and network infrastructure. Completers will learn to manage 250 to 5,000 or more users, multiple physical locations, and multiple domain controllers.

Course Objectives

Course: Microsoft Certified Expert: Microsoft 365 Certified Modern Desktop Administrator Associate

- Deploy Windows
- Manage devices and data
- Configure connectivity
- Maintain Windows
- Deploy and update operating systems
- Manage policies and profiles
- Manage and protect devices
- Manage apps and data

By the end of the course, students will be prepared to pass one or more certification exams, which are designed and administered by Microsoft, and applicable wherever Microsoft technology is used.

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Microsoft Certified Expert:

Microsoft Certified Azure Administrator Associate

Vocational Program

Program Description

Linked to the Microsoft Certified Azure Administrator Associate certification, this course is intended for learners seeking to work as an information technology (IT) professional.

Course Objectives

Course: Microsoft Certified Expert: Microsoft Certified Azure Administrator Associate

- Describe cloud concepts
- Describe Azure architecture and services
- Describe Azure management and governance
- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Implement and manage virtual networking
- Monitor and maintain Azure resources

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

AVOCATIONAL
CERTIFICATE PROGRAMS

These programs vary in length from one to six months, and are intended exclusively for personal or professional development and enhancement.

If you have questions about any of these programs, please contact your Career Specialist.

Please note that not all classes may always be available.

Amazon AWS Certified: Solutions Architect – Associate

Avocational Program

Program Description

The Amazon AWS Certified: Solutions Architect - Associate program covers the fundamentals of building IT infrastructure on Amazon Web Services, or AWS. The course is designed to teach solutions architects how to optimize the use of the AWS Cloud by understanding AWS services and how these services fit into cloud-based solutions. Because architectural solutions can differ depending on industry, type of applications, and size of business, this course emphasizes best practices for the AWS Cloud, and it recommends various design patterns to help you think through the process of architecting optimal IT solutions on AWS. It also presents case studies throughout the course, which showcase how some AWS customers have designed their infrastructures, and the strategies and services that they implemented. Finally, this course also provides opportunities to build a variety of infrastructures via a guided, hands-on approach.

Course Objectives

Course: Amazon AWS Certified: Solutions Architect – Associate

- Describe how cloud adoption transforms the way IT systems work and the benefits of cloud computing with AWS
- Discuss how to design systems that are secure, reliable, high performing, and cost efficient
- Describe principles to consider when migrating or designing new applications for the cloud
- Identify the design patterns and architectural options applied in a variety of use cases
- Define high availability, fault tolerance, and scalability, and discuss how to avoid single points of failure
- List AWS services that have built-in fault tolerance or can be designed for fault tolerance
- Describe why load balancing is key architectural component for AWS-powered applications
- Identify the benefits of Infrastructure as Code
- Describe how to leverage the capabilities of AWS to support automation
- Create, manage, provision, and update related resources using AWS CloudFormation
- Articulate the importance of making systems highly cohesive and loosely coupled
- Describe system coupling to support the distributed nature of applications built for the cloud
- Describe database services for storing and deploying web-accessible
- Compare structured query language—or SQL—databases with NoSQL databases
- Describe how the AWS Well-Architected Framework improves cloud-based architectures
- Describe the business impact of design decisions
- Identify the design principles and best practices of the Operational Excellence pillar
- Describe how to secure data at every layer in the application
- Describe the appropriate tools and services to provide security focused content
- Describe the design principles and the best practices of the Reliability pillar
- Select compute, storage, database, and networking resources to improve performance
- Evaluate the most important performance metrics for your applications; eliminate unneeded costs or suboptimal resources
- Troubleshoot common errors

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Amazon AWS Certified: SysOps Administrator - Associate

Avocational Program

Program Description

The Amazon AWS Certified: SysOps Administrator - Associate program is designed to prepare participants to pursue entry-level DevOps, support, and cloud operations roles. It will also help prepare them to take the AWS SysOps Administrator – Associate exam. Emphasizing best practices in the AWS Cloud and recommended design patterns, this course will teach students how to solve problems and troubleshoot various scenarios. The course will show students how to create automatable and repeatable deployments of networks and systems on AWS and covers specific AWS features and tools related to configuration and deployment. With case studies and demonstrations, students will learn how some AWS customers design their infrastructures and implement various strategies and services. Students will also have the opportunity to build a variety of infrastructures via guided, hands-on activities.

Course Objectives

Course: Amazon AWS Certified: SysOps Administrator – Associate

- Understand AWS infrastructure as it relates to system operations, such as global infrastructure, core services, and account security
- Use the AWS Command Line Interface (AWS CLI), and understand additional administration and development tools
- Manage, secure, and scale compute instances on AWS
- Manage, secure, and scale configurations
- Identify container services and AWS services that are available for serverless computing
- Manage, secure, and scale databases on AWS
- Build virtual private networks with Amazon Virtual Private Cloud (Amazon VPC)
- Configure and manage storage options using the storage services offered with AWS
- Monitor the health of your infrastructure with services such as Amazon CloudWatch, AWS CloudTrail, and AWS Config
- Manage resource consumption in an AWS account by using tags, Amazon CloudWatch, and AWS Trusted Advisor
- Create and configure automated and repeatable deployments with tools such as Amazon Machine Images (AMIs) and AWS CloudFormation

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Certified IT Project Management Expert: Blockchain Analyst

Avocational Program

Program Description

The Certified IT Project Management Expert: Blockchain Analyst program provides students with expert-level understanding of Blockchain technology. Program completers will be prepared to build and secure Blockchain-based applications for businesses; utilize their expertise to make important decisions related to Blockchain projects; and craft the guidelines and structure of the whole Blockchain system considering all system requirements.

This course includes preparation for the industry standard certifications Certified Blockchain Architect, Certified Blockchain Developer, and Certified Blockchain Security Professional.

Course Objectives

Course: Certified IT Project Management Expert: Blockchain Analyst

- Blockchain architecture basics and tools
- Architect your own Blockchain solution
- Understand how to develop solutions using Blockchain, Multichain, Ethereum, Hyperledger, Stellar, and Corda
- Understand Blockchain's inherent security features and associated risks
- In-depth knowledge of best security practices for Blockchain infrastructure
- Understand known Blockchain cyber-attacks
- Differentiate between Blockchain cyber-attacks and threats
- Transfer or mitigate Blockchain security risks

Job Titles That Correlate to This Program

Information Security Analyst, Information Security Administrator, Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Certified IT Project Management Expert: ITIL Foundation

Avocational Program

Program Description

The ITIL Foundation program is an entry level qualification which offers candidates a general awareness of the key elements, concepts and terminology used in the Information Technology Infrastructure Library (ITIL) Service Lifecycle, including the linkages between Lifecycle stages, the processes used and their contribution to Service Management practices. ITIL Foundation is the comprehensive framework upon which IT processes are composed. The ITIL Foundation certification serves as proof that the certified individual understands various IT processes and the relationships that exist between them.

Originally, ITIL was developed by the Central Computer and Telecommunications Agency (CCTA) as a set of comprehensive and interrelated codes of practice. In the IT community, such a code of good practice is extremely useful in terms of achieving the efficient support and delivery of high quality, cost effective IT services.

Upon successful completion of the education and examination components related to this qualification, candidates can expect to gain a general overview, and basic knowledge and understanding of ITIL. Completers will be prepared to enhance the quality of IT service management within an organization.

Course Objectives

Course: Certified IT Project Management Expert: ITIL Foundation

- Service management as a practice (comprehension)
- The ITIL service lifecycle (comprehension)
- Generic concepts and definitions (awareness)
- Key principles and models (comprehension)
- Selected processes (awareness)
- Selected functions (awareness)
- Selected roles (awareness)
- Technology and architecture (awareness)
- Competence and training (awareness)

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	30 Clock Hours (4 Weeks)
Lecture/Lab Hours:	18/12
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,400.00**
Course Materials Fee (nonrefundable):	**$175.00**
Included in Course Materials Fee	
Digital Course Content:	*$25.00*
Virtual Labs:	*$50.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Certified IT Project Management Expert:

PMP/CAPM Project Management Professional

Avocational Program

Program Description

The PMP/CAPM Project Management Professional program is designed to prepare students who currently contribute to project teams in various ways, in a variety of job roles, to advance their careers. The students will move from tasks such as providing subject matter expertise (e.g., marketing, finance, customer care, processing, and fulfillment) and serving as project team sponsors, facilitators, liaisons, or coordinators, to functioning as successful project managers.

Students who complete the PMP/CAPM Project Management Professional program will be prepared to pass either the Project Management Professional (PMP) exam or the Certified Associate in Project Management (CAPM) exam. These are both standardized exams in project management terminology and processes, created and administered by the Project Management Institute (PMI®).

Course Objectives

Course: Certified IT Project Management Expert: PMP/CAPM Project Management Professional

- Define project management fundamentals
- Define project management within the organization
- Define the project management methodology
- Initiate a project
- Develop a project management plan and plan components
- Plan a project schedule
- Plan project costs
- Plan for quality, resources, and procurements
- Plan for risk
- Plan stakeholder engagement and communications
- Execute a project
- Work with stakeholders
- Monitor project work, scope, risks, stakeholder engagement, and communications
- Control project changes, scope, schedule, costs, quality, resources, and procurements
- Close a project

Job Titles That Correlate to This Program

Quality Engineer, Manufacturing Engineer, Project Manager, Process Engineer, Quality Manager, Production Supervisor, Business Analyst, Quality Assurance Manager, Senior Quality Engineer, Senior Project Manager, and other similar titles.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Certified IT Project Management Expert:

Six Sigma Green Belt Certification

Avocational Program

Program Description

Linked with the Six Sigma Green Belt certification, the goal of this program is to provide students with enhanced problem-solving skills, using what is known as the DMAIC Model (Define, Measure, Analyze, Improve, and Control). Students will learn to successfully develop and deploy Six Sigma techniques in leading small-scale improvement projects. They will learn to gather and organize data in support of larger-scale projects, and gain proficiency in Six Sigma statistical tools.

Completers will be prepared to pursue Business Management and Specialist positions in a variety of fields, including but not limited to healthcare, finance, manufacturing, government, or any service or product-based industry.

Course Objectives

Course: Certified IT Project Management Expert: Six Sigma Green Belt Certification

- Discuss the basics of Six Sigma
- Identify Six Sigma methodologies
- Describe the fundamentals of the Define phase
- Describe the fundamentals of project management
- Apply management and planning tools used across the DMAIC methodology to identify opportunities for improvement
- Identify key metrics of a Six Sigma project
- Describe team dynamics
- Identify the basic concepts related to the Measure phase
- Perform basic probability and statistical calculations
- Describe the data collection plan
- Describe descriptive measures of statistics
- Use graphical methods to depict process performance
- Analyze and interpret a measurement system's capability
- Conduct process capability and performance studies
- Describe the fundamentals of the Analyze phase
- Conduct hypothesis testing
- Conduct the Six Sigma Improve phase
- Describe the Control phase of the DMAIC methodology
- Describe SPC
- Describe the implementation of Six Sigma

Job Titles That Correlate to This Program

Quality Engineer, Manufacturing Engineer, Project Manager, Process Engineer, Quality Manager, Production Supervisor, Business Analyst, Quality Assurance Manager, Senior Quality Engineer, Senior Project Manager, and other similar titles.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	66 Clock Hours (1-2 Months)
Lecture/Lab Hours:	40/26
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$2,950.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Cisco Certified Expert: CCNP Enterprise

Avocational Program

Program Description

The Cisco Certified Expert: CCNP Enterprise program prepares students to configure, operate, and troubleshoot large scale enterprise networks. Students will obtain a broad range of skills related to routing, switching, and wireless topics, along with security best practices used in software-driven digital networks. Students will gain practical, hands-on experience preparing them for the CCNP Enterprise certification exams and career-ready skills for professional-level roles in the Information and Communication Technologies (ICT) industry.

Course Objectives

Course: Cisco Certified Expert: CCNP Enterprise

- Wireless (RF, infrastructure, roaming, authenticating, troubleshooting)
- Multicast (concepts, protocols)
- Fabric technologies (SD-Access, SD-WAN)
- Overlay tunnels (IPSec, VXLAN, LISP)
- QoS (mechanisms, applications)
- Security (network access control, threat defense, endpoint and infrastructure security)
- Programmability concepts (APIs, data models, DevNet, GitHub, Python Basics)
- Virtualization concepts (NFV, VMs, virtual switching)
- Automation tools (Embedded Event Manaager, Agent and Agentless tools)
- MPLS Layer 3 VPNs
- Dynamic Multipoint VPN
- DMVPN security
- Advanced BGP
- Troubleshooting IPv6 ACLs
- Flexible Netflow
- Troubleshooting CoPP
- IPv6 First Hop Security
- Cisco DNA Center Assurance

Job Titles That Correlate to This Program

Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	144 Clock Hours (2-4 Months)
Lecture/Lab Hours:	86/58
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$7,500.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cisco Certified Expert: CCNP Collaboration

Avocational Program

Program Description

This program is designed to prepare students to work in the IT field in a variety of positions working with Cisco technologies such as Cisco Routers and Switches, Cisco operating systems, and more. Students will be prepared to obtain the Cisco Certified Network Professional Collaboration certification.

Course Objectives

Course: Cisco Certified Expert: CCNP Collaboration

- Describe the Cisco Collaboration solutions architecture
- Compare the IP Phone signaling protocols of Session Initiation Protocol (SIP), H323, Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP)
- Integrate and troubleshoot Cisco Unified Communications Manager with LDAP for user synchronization and user authentication
- Implement Cisco Unified Communications Manager provisioning features
- Describe the different codecs and how they are used to transform analogue voice into digital streams
- Describe a dial plan, and explain call routing in Cisco Unified Communications Manager
- Implement Public Switched Telephone Network (PSTN) access using MGCP gateways
- Implement a Cisco gateway for PSTN access
- Configure calling privileges in Cisco Unified Communications Manager
- Implement toll fraud prevention
- Implement globalized call routing within a Cisco Unified Communications Manager cluster
- Implement and troubleshoot media resources in Cisco Unified Communications Manager
- Describe Cisco Instant Messaging and Presence, including call flows and protocols
- Describe and configure endpoints and commonly required features
- Configure and troubleshoot Cisco Unity Connection integration
- Configure and troubleshoot Cisco Unity Connection call handlers
- Describe how Mobile Remote Access (MRA) is used to allow endpoints to work from outside the company
- Analyze traffic patterns and quality issues in converged IP networks supporting voice, video, and data traffic
- Define QoS and its models
- Implement classification and marking
- Configure classification and marking options on Cisco Catalyst® switches

Job Titles That Correlate to This Program

Network Administrator, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	301 Clock Hours (4-6 Months)
Lecture/Lab Hours:	181/120
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$7,600.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Cisco Certified Expert: CCNP Data Center

Avocational Program

Program Description

This program is designed to provide students for professional-level job roles in data center technologies. The program focuses on knowledge of data center infrastructure including network, compute, storage network, automation, and security. Students will learn the skills and technologies needed to implement data center computer, LAN and SAN infrastructure, as well as the essentials of automation and security in data centers. Participants gain hands-on experience deploying, securing, operating, and maintaining Cisco data center infrastructure, including Cisco MDS Switches and Cisco Nexus Switches, Cisco Unified Computing System™ (Cisco UCS®) B-Series Blade Servers, and Cisco UCS C-Series Rack Servers.

Program completers will be prepared to obtain the CCNP Data Center certification, which includes a core exam and a concentration exam of the student's choice. Concentration exams are focused on emerging and industry-specific topics such as design, troubleshooting, application-centric infrastructure, storage, and automation.

Course Objectives

Course: Cisco Certified Expert: CCNP Data Center

- Implement routing and switching protocols in Data Center environment
- Implement overlay networks in data center
- Introduce high-level Cisco Application Centric Infrastructure (Cisco ACI™) concepts and Cisco Virtual Machine manager (VMM) domain integration
- Describe Cisco Cloud Service and deployment models
- Implement Fibre Channel fabric
- Implement Fibre Channel over Ethernet (FCoE) unified fabric
- Implement security features in data center
- Implement software management and infrastructure monitoring
- Implement Cisco UCS Fabric Interconnect and Server abstraction
- Implement SAN connectivity for Cisco Unified Computing System™ (Cisco UCS®)
- Describe Cisco HyperFlex™ infrastructure concepts and benefits
- Implement Cisco automation and scripting tools in data center
- Evaluate automation and orchestration technologies

Job Titles That Correlate to This Program

Information Security Analyst, Information Security Administrator, Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	301 Clock Hours (4-6 Months)
Lecture/Lab Hours:	181/120
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$7,600.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cisco Certified Expert: CCNP Security

Avocational Program

Program Description

This program is designed to prepare students to work in the IT field in a variety of positions working with Cisco technologies such as Cisco Routers and Switches, Cisco operating systems, and more. Students will be prepared to obtain the Cisco Certified Network Professional Security certification.

Course Objectives

Course: Cisco Certified Expert: CCNP Security

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication
- Provide basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Job Titles That Correlate to This Program

Information Security Analyst, Information Security Administrator, Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	301 Clock Hours (4-6 Months)
Lecture/Lab Hours:	181/120
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$7,600.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cisco Certified Expert: Cisco Certified CyberOps Associate

Avocational Program

Program Description

This program is designed to validate the day-to-day, tactical knowledge and skills that Security Operations Center (SOC) teams need to prevent, detect, and defend against cybersecurity threats. Students will learn the fundamentals needed for associate-level job roles, including security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents, as well as how to monitor alerts and breaches, and how to understand and follow established procedures for response to incidents. Program completers will be prepared to obtain the Cisco Certified CyberOps Associate certification.

Course Objectives

Course: Cisco Certified Expert: Cisco Certified CyberOps Associate

- Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure the effectiveness of the SOC.
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.
- Describe a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT).
- Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Job Titles That Correlate to This Program

Systems Administrator, Network Administrator, Network Engineer, Information Technology Specialist (IT Specialist), Local Area Network Administrator (LAN Administrator), Information Technology Manager (IT Manager), Information Technology Director (IT Director), Systems Engineer, Network Manager, Network Specialist, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Cisco Certified Expert: Cisco Certified CyberOps Professional

Avocational Program

Program Description

The Cisco Certified Expert: Cisco Certified CyberOps Professional program prepares students to protect, detect, and defend against cybersecurity threats. Students will be guided through cybersecurity operations fundamentals, methods, and automation; learn foundational concepts and their application in real-world scenarios; and obtain the skills needed to meet the increasing demands of the cybersecurity ecosystem, with a focus on intelligent security rather than information security; and gain competency in incident response roles, cloud security, and other active defense security roles.

This course includes preparation for the industry standard certification Cisco Certified CyberOps Professional.

Course Objectives

Course: Cisco Certified Expert: Cisco Certified CyberOps Professional

- Describe the types of service coverage within a SOC and operational responsibilities associated with each.
- Compare security operations considerations of cloud platforms.
- Describe the general methodologies of SOC platforms development, management, and automation.
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, and approaches to each, as part of asset controls and protections.
- Describe Zero Trust and associated approaches, as part of asset controls and protections.
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC.
- Use different types of core security technology platforms for security monitoring, investigation, and response.
- Describe the DevOps and SecDevOps processes.
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Describe API authentication mechanisms.
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response.
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Interpret the sequence of events during an attack based on analysis of traffic patterns.
- Describe the different security tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyze anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

Job Titles That Correlate to This Program

Network Administrator, Network Operation Technician, Network Support, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	144 Clock Hours (2-4 Months)
Lecture/Lab Hours:	86/58
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$7,500.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cisco Certified Expert: Cisco Certified DevNet Associate

Avocational Program

Program Description

This program is designed to provide students with the skills and knowledge necessary for associate-level network automation engineer roles. Students will learn how to implement basic network applications using Cisco platforms as a base; and how to implement automation workflows across network, security, collaboration, and computing infrastructure. Program completers will be prepared to solve real world problems using Cisco Application Programming Interfaces (APIs) and modern development tools.

This course includes preparation for the industry standard certification Cisco Certified DevNet Associate.

Course Objectives

Course: Cisco Certified Expert: Cisco Certified DevNet Associate

- Describe the importance of APIs and use of version control tools in modern software development
- Describe common processes and practices used in software development
- Describe options for organizing and constructing modular software
- Describe HTTP concepts and how they apply to network-based APIs
- Apply Representational State Transfer (REST) concepts to integration with HTTP-based APIs
- Describe Cisco platforms and their capabilities
- Describe programmability features of different Cisco platforms
- Describe basic networking concepts and interpret simple network topology
- Describe interaction of applications with the network and tools used for troubleshooting issues
- Apply concepts of model-driven programmability to automate common tasks with Python scripts
- Identify common application deployment models and components in the development pipeline
- Describe common security concerns and types of tests, and utilize containerization for local development
- Utilize tools to automate infrastructure through scripting and model-driven programmability

Job Titles That Correlate to This Program

Systems Administrator, Network Administrator, Network Engineer, Information Technology Specialist (IT Specialist), Local Area Network Administrator (LAN Administrator), Information Technology Manager (IT Manager), Information Technology Director (IT Director), Systems Engineer, Network Manager, Network Specialist, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Cisco Certified Expert: Cisco Certified Technician (CCT)

Avocational Program

Program Description

This program is designed provide students with the skills to diagnose, restore, repair, and replace critical Cisco networking and system devices at customer sites, preparing them to quickly and efficiently resolve support incidents. The course covers competencies associated with all three Cisco Certified Technician (CCT) certification tracks – Collaboration, Data Center, and Routing and Switching – including onsite support and maintenance of Cisco collaboration endpoints; Cisco Unified computing Systems and servers; and Cisco routers, switches, and operating environments.

Course Objectives

Course: Cisco Certified Expert: Cisco Certified Technician (CCT)

- Use basic Cisco software configuration and tools: CLI commands, Tera Term, Putty, file transfer protocols, USB Storage, serial connections, and Windows
- Describe video and collaboration fundamentals and Cisco collaboration products, including software and hardware components
- Perform remedial services (hardware break/fix) on Cisco collaboration products including software and configuration backup and restore, test calls, software upgrade/downgrade, endpoint resets, and change passwords
- Recognize correct connections and configuration
- Perform basic Layer 1 and basic Layer 2 troubleshooting
- Review Cisco data center networking fundamentals, including SAN, unshielded twisted-pair (UTP) and fiber connectors, the unified computing fabric, and server options.
- Identify Cisco Unified Computing System (Cisco UCS) component models, Cisco Nexus and MDS switches, accessories, cabling, and interfaces.
- Understand Cisco UCS and Cisco Nexus Operating System (Cisco NX-OS) operating modes and identify commonly found software.
- Use the Cisco GUI to connect and service Cisco UCS product components.
- Demonstrate effective field servicing and equipment replacement, and how to troubleshoot most common issues with Cisco UCS servers.
- Use basic Cisco software configuration and tools: Tera Term, Putty, Trivial File Transfer Protocol (TFTP) server, FTP server, USB Storage, loopback plug, and Windows
- Understand network fundamentals, Cisco products, and hardware components
- Perform remedial services (hardware break/fix) on Cisco products including software and configuration backup and restore, software upgrade/downgrade
- Recognize connection type and cable requirement
- Perform basic Layer 1 and basic Layer 2 troubleshooting

Job Titles That Correlate to This Program

Systems Administrator, Network Administrator, Network Engineer, Information Technology Specialist (IT Specialist), Local Area Network Administrator (LAN Administrator), Information Technology Manager (IT Manager), Information Technology Director (IT Director), Systems Engineer, Network Manager, Network Specialist, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

CompTIA Certified Expert: A+

Avocational Program

Program Description

Linked to CompTIA A+ certification, this program is designed to prepare students for technical support and IT operational roles. Program completers will learn to troubleshoot, problem-solve, and understand a wide variety of issues ranging from networking and operating systems to mobile devices and security.

Course Objectives

Course: CompTIA Certified Expert: A+

- Linked to CompTIA A+ Certification
- Identify the components of standard desktop personal computers
- Identify fundamental components and functions of personal computer operating systems
- Identify best practices followed by professional personal computer technicians
- Install and configure computer components
- Identify technical characteristics of system components
- Maintain and troubleshoot peripheral components
- Identify troubleshooting techniques for system component
- Install and configure operating systems
- Maintain and troubleshoot installations of Microsoft Windows
- Identify network technologies
- Support laptops and portable computing devices
- Support printers
- Identify personal computer security concepts
- Install and configure system components
- Troubleshoot system components
- Install and manage network connections
- Support personal computer security

Job Titles That Correlate to This Program

Computer Support Specialist, Helpdesk Support, Desktop Support, Information Technology Specialist (IT Specialist), Support Specialist, Computer Technician, Help Desk Analyst, Technical Support Specialist, Network Support Specialist, Network Technician, Computer Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$2,875.00**
Course Materials Fee (nonrefundable):	**$400.00**
Included in Course Materials Fee	
Digital Course Content:	***$100.00***
Virtual Labs:	***$150.00***
Practice Tests:	***$100.00***
eBooks:	***$50.00***

CompTIA Certified Expert: Data Cabling Installer

Avocational Program

Program Description

Linked to the ETA Low Voltage Cabling certification. Learners gain hands-on knowledge and ability to successfully conduct site surveys, pull wire/cable and terminate and test copper to the highest level of specification (currently Category 6). The program offers core skills training to meet the diverse needs of the telecommunications cabling industry.

Course Objectives

Course: CompTIA Certified Expert: Data Cabling Installer

- Installation of cables –CAT5 and fiber optics
- Basic wiring to make connection-point moves across rooms
- Troubleshoot and locate   existing cabling; terminate and label cabling
- Server break/fix; racking and stacking servers
- Switches; cabling from server to patch panel

Job Titles That Correlate to This Program

Cable repair technician, Central Office Technician, Install / Repair Technician, Service Technician, Installer, Telecommunications Technician, Customer Service Technician (CST), Combination Technician, Field Technician, Communications Technician, Outside Plant Technician, and other similar titles.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$4,500.00**
Course Materials Fee (nonrefundable)**:**	**$0.00**

CompTIA Certified Expert: Linux+

Avocational Program

Program Description

Participants who complete the CompTIA Certified Expert: Linux+ program will acquire the skills needed to install and support one or more distributions of the Linux operating system and learn information and skills that will be helpful as you prepare for LPI exams.

This course is intended for entry-level computer support professionals with basic knowledge of computer hardware, software, and operating systems, who wish to increase their knowledge and understanding of Linux concepts and skills to prepare for a career in Linux support or administration, or to prepare for LPI exams. A typical student in the Linux+ program should have at least 6 to 12 months of Linux experience.

Course Objectives

Course: CompTIA Certified Expert: Linux+

- Perform basic Linux tasks
- Manage users and group
- Manage permissions and ownership
- Manage storage
- Manage files and directories
- Manage kernel modules
- Manage the Linux boot process
- Manage system components
- Manage devices
- Manage networking
- Manage packages and software
- Secure Linux systems
- Write and execute Bash shell scripts
- Automate tasks
- Plan and perform a Linux installation

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Cybersecurity Certified Expert: Certified Ethical Hacker (CEH)

Avocational Program

Program Description

The Certified Ethical Hacker program is designed to immerse students in an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The Ethical Hacker is an individual who is usually employed with an organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems of that organization using the same methods and techniques as a hacker.

Covering 20 of the most current security domains any ethical hacker will need to know in order to increase the information security posture of their organization, the program's objective is to educate, introduce and demonstrate hacking tools and hacking methodology for penetration testing purposes or ethical hacking situations. The program is structured around the real-life ethical hacking methodology beyond automated vulnerability scans and simple information security tests, using real-time information security incidents and cases to inculcate a capability of making knowledgeable decisions while defending your organization's information resources.

Course Objectives

Course: Cybersecurity Certified Expert: Certified Ethical Hacker (CEH)

- Understanding how perimeter defenses work
- Scanning and attacking students' own networks (no real network is harmed)
- Understanding how intruders escalate privileges
- Securing various systems against intrusion
- Understanding Intrusion Detection, Policy Creation, Social Engineering, DDos Attacks, Buffer Overflows, and Virus Creation
- Preparation Certified Ethical Hacker exam 312-50

Legal Agreement

The Certified Ethical Hacker program mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, students will be asked to sign an agreement stating that they will not use the newly acquired skills for illegal or malicious attacks, nor will they use such tools in an attempt to compromise any computer system. Students must agree to indemnify Lab Four with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Job Titles That Correlate to This Program

Information Security Analyst, Network Operation Technician, Web Developer, Network Support Technician, Computer Network Architect, Computer Network Support Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	At least 2 years of information security related experience
Tuition for Program:	**$3,850.00**
Course Materials Fee (nonrefundable)**:**	**$570.00**
Included in Course Materials Fee	
Digital Course Content:	***$100.00***
Virtual Labs:	***$320.00***
Practice Tests:	***$125.00***
eBooks:	***$25.00***

Cybersecurity Certified Expert:

Certified Information Systems Security Professional (CISSP)

Avocational Program

Program Description

Completers of the Certified Information Systems Security Professional program will be firmly grounded in the knowledge requirements of today's security professional. This program will address the essential elements of the eight domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals. The program offers a job-related approach to the security process, while providing a framework to prepare for CISSP certification.

CISSP is the premier certification for today's information systems security professional. It remains the premier certification because the sponsoring organization, the International Information Systems Security Certification Consortium, Inc. (ISC)2 ®, regularly updates the test by using subject matter experts (SMEs) to make sure the material and the questions are relevant in today's security environment. By defining eight security domains that comprise a CBK, industry standards for the information systems security professional have been established. The skills and knowledge participants gain in this program will help them master the eight CISSP domains and ensure their credibility and success within the information systems security field.

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career. Through the study of all eight CISSP Common Body of Knowledge (CBK) domains, students will validate their knowledge by meeting the necessary preparation requirements to qualify to sit for the CISSP certification exam.

Additional CISSP certification requirements include a minimum of five years of direct professional work experience in two or more fields related to the eight CBK security domains, or a college degree and four years of experience. It is highly recommended that students have certifications in Network+ or Security+, or possess equivalent professional experience upon entering CISSP training. It will be beneficial if students have one or more of the following security-related or technology-related certifications or equivalent industry experience: CyberSec First Responder (CFR) MCSE, CCNP, RHCE, LCE, SSCP®, GIAC, CISA™, or CISM®.

Course Objectives

Course: Cybersecurity Certified Expert: Certified Information Systems Security Professional (CISSP)

- Analyze components of the Security and Risk Management domain.
- Analyze components of the Asset Security domain.
- Analyze components of the Security Engineering domain.
- Analyze components of the Communications and Network Security domain.
- Analyze components of the Identity and Access Management domain.
- Analyze components of the Security Assessment and Testing domain.
- Analyze components of the Security Operations domain.
- Analyze components of the Software Development Security domain.

Job Titles That Correlate to This Program

Information Security Analyst, Network Operation Technician, Web Developer, Network Support Technician, Computer Network Architect, Computer Network Support Specialist, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	(to be eligible for CISSP exam) Minimum 5 years professional experience in information security. Work history must show skill set embraces at least 2/10 domains in the (ISC)^2 CISSP Common Body of Knowledge (CBK)
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Microsoft Certified Expert:

Microsoft 365 Certified Security Administrator Associate

Avocational Program

Program Description

This program will prepare students to work in the IT field in a variety of positions working with Microsoft technologies. Students will be prepared to obtain the Microsoft 365 Certified Security Administrator Associate certification.

Course Objectives

Course: Microsoft Certified Expert: Microsoft 365 Certified Security Administrator Associate

- Implement and manage identity and access
- Secure Microsoft 365 hybrid environments
- Implement authentication methods
- Implement conditional access
- Implement role-based access control (RBAC)
- Implement Azure AD Privileged Identity Management (PIM)
- Implement Azure AD Identity Protection
- Implement and manage threat protection
- Implement an enterprise hybrid threat protection solution
- Implement device threat protection
- Implement and manage device and application protection
- Implement and manage Microsoft Defender for Office 365
- Implement and manage information protection
- Secure data access within Office 365
- Implement and manage Microsoft Cloud App Security
- Manage governance and compliance features in Microsoft 365
- Configure and analyze security reporting
- Manage and analyze audit logs and reports
- Manage data governance and retention
- Manage search and investigation
- Manage data privacy regulation compliance

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	1-3 years of IT/IT Support experience recommended
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Microsoft Certified Expert:

Microsoft Certified Azure Database Administrator Associate

Avocational Program

Program Description

This program prepares participants to implement and manage the operational aspects of cloud-native and hybrid data platform solutions built with Microsoft SQL Server and Microsoft Azure Data Services. Students will learn to plan and implement data platform resources; implement a secure environment; perform automation of tasks; plan and implement a High Availability and Disaster Recovery (HADR) environment; and perform administration by using T-SQL.

This course includes preparation for the industry standard certification Microsoft Certified Azure Database Administrator Associate.

Course Objectives

Course: Microsoft Certified Expert: Microsoft Certified Azure Database Administrator Associate

- Plan and implement data platform resources
- Implement a secure environment
- Monitor and optimize operational resources
- Optimize query performance
- Perform automation of tasks
- Plan and implement a High Availability and Disaster Recovery (HADR) environment
- Perform administration by using T-SQL

Job Titles That Correlate to This Program

Database Administrator, Database Analyst, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	1-3 years of experience as a Database Administrator recommended
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Microsoft Certified Expert:

Microsoft Certified Azure Security Engineer Associate

Avocational Program

Program Description

The Microsoft Certified Expert: Microsoft Certified Azure Security Engineer Associate program prepares students to implement security controls and threat protection, manage identity and access, and protect data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure. Students will learn to use a variety of security tools to maintain the security posture, identify and remediate vulnerabilities, implement threat protection, and respond to security incident escalations.

This course includes preparation for the industry standard certification Microsoft Certified: Azure Security Technologies.

Course Objectives

Course: Microsoft Certified Expert: Microsoft Certified Azure Security Engineer Associate

- Manage identity and access
- Implement platform protection
- Manage security operations
- Secure data and applications

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Blended
Delivery Mode(s):	Residential (on-campus); or Interactive Distance Learning (online)
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	None
Recommended:	1-3 years of experience as a Database Administrator recommended
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

Microsoft Certified Expert:

Microsoft Certified Cloud Developer (C# and .NET)

Avocational Program

Program Description

This program will prepare students to work in the IT field in a variety of positions working with Microsoft technologies. Students will be prepared to obtain the Microsoft Certified Cloud Developer certification.

Course Objectives

Course: Microsoft Certified Expert: Microsoft Certified Cloud Developer (C# and .NET)

- Fundamentals of HTML
- Interactivity using JavaScript
- HTTP servers
- Rest API
- HTTP services
- CSS fundamentals
- Python
- MEAN stack
- MongoDB (NoSQL)
- Python Django
- NodeJS
- ReactJS
- Quality and Performance
- Devops, etc.

Job Titles That Correlate to This Program

Software Engineer, Application Integration Engineer, Programmer Analyst, Software Development Engineer, Computer Consultant, Software Architect, Software Developer, Technical Consultant, Applications Developer, Business Systems Analyst, Programmer Analyst, Programmer, Analyst Programmer, Computer Programmer, Software Developer, Applications Developer, Computer Programmer Analyst, Internet Programmer, Java Developer, Web Programmer, , Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	301 Clock Hours (4-6 Months)
Lecture/Lab Hours:	181/120
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	1-3 years of experience in the IT field recommended
Tuition for Program:	**$7,600.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Microsoft Certified Expert:

Microsoft Certified Security Operations Analyst

Avocational Program

Program Overview

This program will prepare students to secure information technology systems for their organization, with the goal of reducing organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Students will gain an understanding of threat management, monitoring, and response by using a variety of security solutions across their environment; and program completers will be prepared to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products.

This course includes preparation for the industry standard certification Microsoft Certified: Security Operations Analyst Associate.

Course Objectives

Course: Microsoft Certified Expert: Microsoft Certified Security Operations Analyst

- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Mitigate threats using Azure Sentinel

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	301 Clock Hours (4-6 Months)
Lecture/Lab Hours:	181/120
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Recommended:	1-3 years of experience with Windows Server in an enterprise environment
Tuition for Program:	**$7,600.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	***$50.00***
Virtual Labs:	***$100.00***
Practice Tests:	***$75.00***
eBooks:	***$25.00***

Microsoft Certified Expert: VMware Certified Associate

Avocational Program

Program Description

The VMware Certified Associate Boot Camp program is designed to prepare students to pass the VMware Certified Associate certification exam and to attain entry level System Administration positions that require exposure to virtual infrastructure technologies. VMware certification is the most widely recognized certification in the virtualization industry, and as physical datacenters are becoming software defined datacenters, Systems Administrators with virtualization skills are in high demand. Students will learn the fundamental building blocks of VMware's vSphere data center virtualization technology, setting the foundation for a career as a certified professional and being able to manage small, medium, and large scale virtual infrastructures.

The program features intensive hands-on training that focuses on installing, configuring, and managing VMware vSphere® 6, which includes VMware ESXi™ 6 and VMware vCenter Server™ 6. This program will give students a solid understanding of how to administer a vSphere infrastructure for an organization of any size.

Course Objectives

Course: Microsoft Certified Expert: VMware Certified Associate

- Describe the software-defined data center
- Deploy an ESXi host and create virtual machines
- Describe vCenter Server architecture
- Deploy a vCenter Server instance or VMware vCenterServer™ Appliance™
- Use vCenter Server to manage an ESXi host
- Configure and manage vSphere infrastructure with VMware vSphere® Client™ and VMware vSphere® Web Client
- Configure virtual networks with vSphere standard switches
- Use vCenter Server to manage various types of host storage: VMware vSphere® VMFS, NFS, virtual SAN, and Virtual Volume
- Manage virtual machines, templates, clones, and snapshots
- Create a vApp
- Migrate virtual machines with VMware vSphere® vMotion®
- Use VMware vSphere® Storage vMotion® to migrate virtual machine storage
- Monitor resource usage and manage resource pools
- Introduce VMware vRealize™ Operations Manager™ to identify and solve issues through analytics and alerts
- Manage VMware vSphere® High Availability and VMware vSphere® Fault Tolerance
- Understand VMware vSphere® Replication™ and VMware vSphere® Data Protection™ to replicate virtual machines and perform data recovery
- Use VMware vSphere® Distributed Resource Scheduler™ clusters to improve host scalability
- Learn about vSphere distributed switches to improve network scalability
- Understand VMware vSphere® Update Manager™ to apply patches and perform basic troubleshooting of ESXi hosts, virtual machines, and vCenter Server operations
- VMware Testing and Certification Readiness

Job Titles That Correlate to This Program

Server Administrator, Systems Administrator, Network Administrator, Systems Engineer, Network Operation Technician, Network Support Specialist, Network Support Technician, Network Technician, Computer Support Specialist, Helpdesk Support, Desktop Support, or other similar jobs.

Learning Methodology:	Residential
Delivery Mode(s):	Residential (on-campus) only
Credential Awarded:	Certificate of Completion
Length of Program:	72 Clock Hours (1-2 Months)
Lecture/Lab Hours:	43/29
Maximum Student/Teacher Ratio	25:1
Withdrawal Fee:	$100.00
Prerequisites:	Either 1 year relevant work experience, 1 year postsecondary education at an accredited institution in a related field, or 1 industry certification in a related field
Tuition for Program:	**$3,750.00**
Course Materials Fee (nonrefundable):	**$250.00**
Included in Course Materials Fee	
Digital Course Content:	*$50.00*
Virtual Labs:	*$100.00*
Practice Tests:	*$75.00*
eBooks:	*$25.00*

APPENDIX 1

COMPUTER USAGE AND INTERNET AUTHORIZATION

I have read the Student Internet Acceptable Use Policy. I understand and will abide by the Student Internet Acceptable Use Policy. I understand that access is designed for educational purposes. I understand any violations of the above provisions will result in the loss of my Internet access privilege, and may result in further disciplinary action and/or legal action, including but not limited to suspension or expulsion, or referral to legal authorities.

____

Student Name (print)

____

Student Signature **Date**

APPENDIX 2

STUDENT COMMITMENT TO EXCELLENCE

As a student at Lab Four, I understand the following to be the guidelines both for my own growth and development as a student and my commitment to excellence.

□ I understand that my role as a student at Cybersecurity Institute at Lab Four is a significant responsibility, and I will make it a priority during the time that I am enrolled in the program. I also agree to maintain active and meaningful academic participation including learning and conceptualizing the material that is taught in class and asking questions when I am unsure if I understand the material. I will use all available resources including my instructor, my book, practice tests, and any other reasonable materials to assist me with course material.

□ I will participate in class discussions and attend every class session. I understand that if I miss class in excess, disciplinary actions may be taken against me, per the published Attendance Policy. If I know in advance that I will be absent from a class session, I will inform my instructor in a timely manner.

□ I will be respectful of the professional learning environment at Lab Four. I understand that disciplinary actions may be taken against me if I am found in violation of the published Student Conduct Policy.

□ I understand that I must be in good standing with Lab Four's Satisfactory Academic Progress, Student Conduct, and Attendance Policies, as well as having no outstanding documentation or financial balance, in order for Lab Four to cover or contribute to the cost of any certification exam applicable to my program. I also understand that beyond 120 days after class completion, Lab Four will not cover the cost of any exam attempt regardless of my eligibility prior to that date.

□ I understand that I will have access to Lab Four Support Services for up to one year after successful completion of my approved training program, provided that eligibility requirements are met. The support services include access to the practice test, ability to audit the class that I completed, and Employment and Entrepreneurship Assistance Services.

□ I understand that I must participate in Employment and Entrepreneurship Assistance Services (EEAS) activities, meeting all assigned EEAS Deadlines in order for the EEAS Specialist to submit my resume for any position. I also understand that if I fail to participate in EEAS activities, I may not be considered for job placement services.

□ I understand that academic dishonesty is strictly prohibited. This includes, but is not limited to cheating on tests, falsifying attendance records, plagiarism, and collusion.

I acknowledge that I have received a copy of the Student Handbook. I understand that I am responsible for becoming familiar with its contents. The policies and procedures are included in the handbook to hopefully eliminate unnecessary confusion during the time I am enrolled, and after. I also acknowledge that I have read the above guidelines and I agree to abide by them.

____

Student Name (print)

____

Student Signature **Date**

APPENDIX 3

IDL Student Disclosure

The Interactive Distance Learning (IDL) option at Lab Four allows students to attend classes in a live, instructor-led, interactive "classroom" environment from the comfort of their own home. This delivery methodology includes all the support students would experience on campus, and is designed to help students achieve their goals. Resources include virtual practice labs, video lessons and post-assessments, practice tests, eBooks, tutoring and hands-on workshops offered outside of class time, instructors with real-world experience in what they teach, and a dedicated Employment and Entrepreneurship Assistance Services (EEAS) team.

Please read carefully and initial the following statements:

________ To participate in an IDL program, I understand that I must have the following:

1. A computer
2. Internet access
3. A webcam or cell phone camera that can be connected to your computer (for video)
4. Headphones or speakers that can be connected to your computer (for audio)
   (alternatively, each class session will have a unique conference call number you can call into for audio once you join)

________ I understand that Lab Four does not include or pay for internet access. I am aware that I am required to supply my own internet access in order to participate in the IDL program.

________ I understand that the IDL program requires internet speeds of at least 2 Mbps, and wired connections are preferred. Hotspots, cell phone internet service, and dial-up connections are insufficient.

________ I understand that I must furnish my own working laptop or desktop computer in order to participate in the IDL program.

________ I understand that I am expected to attend classes during my scheduled class time, as identified in my course syllabus and enrollment agreement.

________ I understand that I must attend a New Student Orientation and live demonstration in Microsoft Teams for Education prior to the start of my classes. I will not be able to start the program if I do not attend the orientation session.

By signing below, I am confirming that I understand and accept the requirements associated with the interactive distance learning (IDL) program.

Student Signature: ________________________________ **Date:** ____________________

APPENDIX 4

Program Completion and Reward Redemption

This document includes all the milestones and rewards associated with completion of a Lab Four program, as well as how to claim them when you qualify. Qualifications for rewards vary slightly depending on whether you are participating in a performance-based funding program (or your tuition and fees are otherwise not paid in full as of the program completion date); versus if you have no outstanding balance on your tuition and fees upon program completion. **Please be sure to consult the appropriate section of this form for the rewards that apply to you. If you are unsure, please inquire via email to help@labfour.edu.**

All Students

The milestones and rewards listed in this section apply to all students, regardless of funding status.

Best in Class Professional (BCP)

Any student can earn Lab Four's Best in Class Professional (BCP) recognition after program completion. Those qualifications are as follows:

- 90% Attendance and 90% Cumulative Grade (or higher)
- Have obtained at least one certification within 90 days after completion
- Start a business, start a job, or secure a promotion within 90 days after completion
    - Must be in a position supported by your program of study
    - All required meaningful employment documentation must be complete and meaningful employment must be *verified*, meaning Lab Four must confirm the student has worked at least 30 days in the position following class completion.

Graduation Gift

To commend you for your hard work, Lab Four offers a graduation gift to successful program completers.* Students must meet the following qualifications to receive a graduation gift:

- Complete your training program with a minimum attendance rate of 80% and a minimum cumulative grade of 70%
- Have no outstanding documentation or tuition/fee balance
- *If you are in a vocational program, you must also have obtained a training-related employment or entrepreneurship outcome, complete with all required meaningful employment documentation within four months (120 days) after the class end date.*
    - Required supporting documentation for a meaningful employment outcome may include an offer letter and/or pay stub(s). Business owners must submit 1) proof of ownership of the business (e.g. Federal Tax ID/EIN, business license/registration, Articles of Incorporation, etc.); 2) marketing material showing the scope or level or services offered; and 3) proof of legitimate business transactions (a bill and payment from a client that displays the type of services being provided and/or products sold).
    - Meaningful employment must also be *verified*, meaning Lab Four must confirm the student has worked at least 30 days in the position following class completion.

Graduation gifts vary depending upon the length of the program.
→ **Students who complete a program less than 600 clock hours** may choose between a $50.00 Apple or Samsung gift certificate.
→ **Students who complete a program 600 clock hours or more** may choose between a base model Apple Watch, AirPods, Samsung Galaxy Buds, or Galaxy Watch. Depending on the product, this gift may be facilitated in the form of a gift card instead of the physical item. The gift card will cover the full price of the base model item, taxes, and shipping.

HOW TO CLAIM: Complete the *Graduation Gift Confirmation Form* to choose which device you would like and confirm your address for shipment or email for gift card fulfillment. We will send you the electronic form via email when the qualifications are met.

Graduation gifts will not be shipped until all meaningful employment documentation has received final approval from all relevant parties, including Lab Four and any government entity that provided funding for your training, if applicable.

Continued Support and Post-Completion Resources

After your instructor-led classes have ended, Lab Four provides continued support through the following:

- Four months (120 days) continued access to Practice Exams, Skillsoft, Microsoft Teams for Education, and weekly Hands-On, Tutoring, and Employment and Entrepreneurship Assistance Services (EEAS) and EEAS Workshops for those who have remained actively engaged in the pursuit of certification and meaningful employment outcomes, or who have already achieved a meaningful employment outcome.
    - If you have not yet achieved a meaningful employment outcome complete with all required documentation, you must engage with one or more of the continuing academic or EEAS resources (at least twice per month) to maintain eligibility. Sign up for tutoring sessions, EEAS coaching sessions, resume assistance, mock interviews, or other workshops **here**.

  - *Extensions beyond the 120 days immediately following the class end date may be requested via email to help@labfour.edu and will be reviewed and approved on a case-by-case basis.*
- Successful program completers* have access to audit any course you've completed for up to one year after your completion date.
- Official Transcripts and Certificates of Completion can be requested via email to help@labfour.edu and will be released only to those who do not have any outstanding documentation or outstanding tuition or fee balance.

The term "successful program completer" refers to individuals who have met the course completion requirements, as well as achieved an approved training-related employment or entrepreneurship outcome complete with all documentation required by both Lab Four and any government entity that provided funding for your training, if applicable, and have no outstanding tuition or fee balance.

Students with <u>NO</u> Outstanding Tuition/Fee Balance Upon Program Completion

If the total tuition and fees for your training program are paid in full – whether you submitted payment in full prior to enrollment; participated in a scholarship or grant program that covers the full tuition and fees for your program up front; or enrolled in a payment plan and have paid off your balance – the following qualifications and reward redemption instructions apply to you.

Exam Vouchers

To receive any exam vouchers, students must meet the following qualifications:

- Be in good standing with Lab Four's Satisfactory Academic Progress (SAP) Policy (minimum 70% cumulative grade)
- Be in good standing with Lab Four's Attendance Policy (minimum 80% attendance rate)
- Be in good standing with Lab Four's Student Conduct policy
- Have no outstanding documentation
- *If you are in a vocational program, you must also have successfully completed EEAS Checkpoint Assignments in order to be issued any exam vouchers*. Meaningful employment must also be *verified*, meaning Lab Four must confirm the student has worked at least 30 days in the position following class completion.

→ **For those enrolled in a program <u>less than 600 clock hours</u> in length**, Lab Four will contribute up to **$325.00** toward the first attempt at *each certification associated with your program*. All vouchers must be both earned and used within four months (120 days) after program completion.

- <u>HOW TO QUALIFY</u>: You must meet program *completion* requirements (min. 70% grade; min. 80% attendance) <u>and</u> if you are enrolled in a vocational program you must also have completed your EEAS Checkpoint Assignments, or received a waiver for EEAS Checkpoint Assignments, if applicable.
- <u>HOW TO CLAIM</u>: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use an exam voucher.

→ **For those enrolled in a program that is <u>600 or more clock hours</u> in length,** Lab Four provides **three** opportunities for you to receive exam vouchers, not to exceed **$325.00** in value per voucher. All vouchers must be both earned and used within six months (180 days) after program completion.

Voucher #1:

- <u>HOW TO QUALIFY</u>: Successfully complete Modules 1 and 2 (min. 70% grade; min. 80% attendance) <u>and</u> have successfully completed <u>all</u> EEAS Checkpoint Assignments to date or received waivers for EEAS Checkpoint Assignments, if applicable.
- <u>HOW TO CLAIM</u>: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your first exam voucher.
- <u>NOTE</u>: Vouchers #2 and #3 may <u>not</u> be used to retake the exam for which voucher #1 was issued, should you not pass.

Voucher #2:

- <u>HOW TO QUALIFY</u>: Successfully complete all modules (min. 70% grade; min. 80% attendance) <u>and</u> have successfully completed <u>all</u> EEAS Checkpoint Assignments, or received waivers for EEAS Checkpoint Assignments, if applicable.
- <u>HOW TO CLAIM</u>: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your second exam voucher.

Voucher #3:

- <u>HOW TO QUALIFY</u>: Meet the *Best in Class Professional (BCP)* criteria described above (page 1 of this document).
- <u>HOW TO CLAIM</u>: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your third exam voucher.

Students WITH an Outstanding Tuition/Fee Balance Upon Program Completion

If the total tuition and fees for your training program are not paid in full upon program completion – whether you participated in a funding program with a performance-based payment structure; or enrolled in a payment plan and have not yet paid off your balance – the following qualifications and reward redemption instructions apply to you.

Exam Vouchers

To receive any exam vouchers, students must meet the following qualifications:

- Be in good standing with Lab Four's Satisfactory Academic Progress (SAP) Policy (minimum 70% cumulative grade)
- Be in good standing with Lab Four's Attendance Policy (minimum 80% attendance rate)
- Be in good standing with Lab Four's Student Conduct policy
- Have no outstanding documentation
- *If you are in a vocational program, you must also have obtained a training-related employment or entrepreneurship outcome, complete with all required meaningful employment documentation.*
  - Required supporting documentation for a meaningful employment outcome may include an offer letter and/or pay stub(s). Business owners must submit 1) proof of ownership of the business (e.g. Federal Tax ID/EIN, business license/registration, Articles of Incorporation, etc.); 2) marketing material showing the scope or level or services offered; and 3) proof of legitimate business transactions (a bill and payment from a client that displays the type of services being provided and/or products sold).
  - Meaningful employment must also be *verified*, meaning Lab Four must confirm the student has worked at least 30 days in the position following class completion.
  - **No exam vouchers will be issued until all meaningful employment documentation has received final approval from all relevant parties, including Lab Four and any government entity that provided funding for your training, if applicable.**

→ **For those enrolled in a program less than 600 clock hours in length**, Lab Four will contribute up to **$325.00** toward the first attempt at *each certification associated with your program*. All vouchers must be both earned and used within four months (120 days) after program completion.

- HOW TO QUALIFY: You must meet program *completion* requirements (min. 70% grade; min. 80% attendance) and if you are enrolled in a vocational program you must also have obtained a training-related meaningful employment or entrepreneurship outcome, complete with all required documentation.
- HOW TO CLAIM: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your first exam voucher.

→ **For those enrolled in a program that is 600 or more clock hours in length,** Lab Four provides **three** opportunities for you to receive exam vouchers, not to exceed **$325.00** in value per voucher. All vouchers must be both earned and used within six months (180 days) after program completion.

Voucher #1:

- HOW TO QUALIFY: Successfully complete Modules 1 and 2 (min. 70% grade; min. 80% attendance) and obtain a training-related meaningful employment or entrepreneurship outcome, complete with all required documentation.
- HOW TO CLAIM: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your first exam voucher.
- NOTE: Vouchers #2 and #3 may not be used to retake the exam for which voucher #1 was issued, should you not pass.

Voucher #2:

- HOW TO QUALIFY: Successfully complete all modules (min. 70% grade; min. 80% attendance) and obtain a training-related meaningful employment or entrepreneurship outcome, complete with all required documentation.
- HOW TO CLAIM: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your second exam voucher.

Voucher #3:

- HOW TO QUALIFY: Meet the *Best in Class Professional (BCP)* criteria described above (page 1 of this document).
- HOW TO CLAIM: Call 901-261-1111 or email help@labfour.edu with the subject line "Voucher Request" to let us know which certification exam you would like to take, and that you would like to use your third exam voucher.

APPENDIX 5

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) affords eligible students certain rights with respect to their education records. (An "eligible student" under FERPA is a student who is 18 years of age or older or who attends a postsecondary institution at any age.) These rights include:

1. The right to inspect and review the student's education records within 45 days after the day Lab Four [“School” or “Institution”] receives a request for access. A student should submit to the registrar, dean, head of the academic department, [or other appropriate official,] a written request that identifies the record(s) the student wishes to inspect. The school official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the school official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

2. The right to request the amendment of the student’s education records that the student believes is inaccurate, misleading, or otherwise in violation of the student’s privacy rights under FERPA.

   A student who wishes to ask the school to amend a record should write the school official responsible for the record, clearly identify the part of the record the student wants changed, and specify why it should be changed.

   If Lab Four decides not to amend the record as requested, Lab Four will notify the student in writing of the decision and the student’s right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

3. The right to provide written consent before Lab Four discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

   Lab Four discloses education records without a student’s prior written consent under the FERPA exception for disclosure to school officials with legitimate educational interests. A school official is typically includes a person employed by the Institution in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person serving on the board of trustees; or a student serving on an official committee, such as a disciplinary or grievance committee. A school official also may include a volunteer or contractor outside of the Institution who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, or collection agent or a student volunteering to assist another school official in performing his or her tasks. A school official typically has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the Institution.

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the Institution to comply with the requirements of FERPA. The name and address of the office that administers FERPA is:

   Family Policy Compliance Office
   U.S. Department of Education
   400 Maryland Avenue, SW
   Washington, DC 20202

FERPA permits the disclosure of PII from students’ education records, without consent of the student, if the disclosure meets certain conditions found in § 99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the student, § 99.32 of FERPA regulations requires the institution to record the disclosure. Eligible students have a right to inspect and review the record of disclosures. A postsecondary institution may disclose PII from the education records without obtaining prior written consent of the student —

- To other school officials, including teachers, within the Institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in § 99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(3) are met. (§ 99.31(a)(1))
- To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of § 99.34. (§ 99.31(a)(2))
- To authorized representatives of the U. S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising the university's State-supported education programs. Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§ 99.31(a)(3) and 99.35)
- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§ 99.31(a)(4))
- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§ 99.31(a)(6))
- To accrediting organizations to carry out their accrediting functions. (§ 99.31(a)(7))
- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§ 99.31(a)(8))
- To comply with a judicial order or lawfully issued subpoena. (§ 99.31(a)(9))
- To appropriate officials in connection with a health or safety emergency, subject to § 99.36. (§ 99.31(a)(10))
- Information the school has designated as "directory information" under § 99.37. (§ 99.31(a)(11))
- To a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense, subject to the requirements of § 99.39. The disclosure may only include the final results of the disciplinary proceeding with respect to that alleged crime or offense, regardless of the finding. (§ 99.31(a)(13))
- To the general public, the final results of a disciplinary proceeding, subject to the requirements of § 99.39, if the school determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the student has committed a violation of the school's rules or policies with respect to the allegation made against him or her. (§ 99.31(a)(14))
- To parents of a student regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the school, governing the use or possession of alcohol or a controlled substance if the school determines the student committed a disciplinary violation and the student is under the age of 21. (§99.31(a)(15))

APPENDIX 6

Recordkeeping Policy and Procedure

Student Record Retention

All student records must be maintained in a manner that provides (1) access for authorized faculty and staff to carry out their normal job responsibilities, (2) reasonable protection against misplacement, loss, destruction, or theft, and (3) organized availability for third party review. Confidential or sensitive records should be stored in a secure location with locking filing cabinets, in an office that remains locked when not in use. Unless authorized by a member of senior management, student records must be stored on the premises (including approved off-site storage facilities) at all times.

Records should be maintained in an environment that is free from vermin, flooding, fire hazards, and unusual amounts of moisture, and heat. Ideally, this area would be continuously monitored for fires, water intrusion, and fluctuations in temperature or humidity outside these established standards.

All student records are kept for a minimum of three years, unless otherwise noted. This includes, but is not limited to:

Admissions Correspondence	3 years
Applications – admitted and enrolled	3 years following the completion or withdrawal date
Applications – admitted but not enrolled	1 year
Applications – not admitted	1 year
Incomplete Application files	1 year
Readmission Applications	3 years
Residency Classification Files	3 years
Applications (Financial Aid)	3 years
Financial Aid Transcripts	Permanently
Scholarships	3 years
Academic Records	Permanently
Changes of Course (e.g., drop/add rolls)	1 year
Correspondence	3 years
Family Educational Rights and Privacy Act (FERPA) Documents	Life of affected record (i.e., the same retention period as that of the student record to which it pertains)
Final Grade Rolls	Permanently
Loan Deferment Certifications	3 years
Supplemental Grade Changes	Permanently
Transcript Requests	3 years
Veterans' Records	3 years
Withdrawal Applications	3 years
Withdrawal Authorization Forms	3 years

THEC Requirements

Certificates of Completion	Permanently
Official Complaints	3 years
Any other Financial Documentation	3 years

Applicant and Student Record Creation and Auditing

Effective July 1, 2020, all Applicant and Student records are created, stored, and maintained electronically. The Enrollment Team is responsible for the creation and maintenance of Applicant Records prior to Enrollment. To ensure that admission requirements are satisfied and all necessary documentation is in place prior to enrollment, Career Specialists must follow the appropriate *Student File Checklist* (Application section) when assembling Applicant Files.

Once the Application section of the *Student File Checklist* are complete, the Applicant File is submitted to the Registration Manager for approval prior to enrollment. The Registration Manager or designee will audit the electronic file and return it to the Career Specialist if corrections are needed. Once the Applicant file is approved, it is marked as such on the *Student File Audit Report* and the Applicant is marked as admitted on the appropriate pending class roster(s). Any hard copy documents, such as official high school transcripts or GED scores collected to document the basis for admission, are organized by application date and stored in a lockable filing cabinet, in an office that remains locked when not in use.

Upon receipt of funding approval (or, if the student is self-pay, upon receipt of their tuition payment) and confirmation that the Applicant File is complete and approved, the student is scheduled for orientation and the Enrollment and Registration documents are generated. These documents make up the Enrollment section of the *Student File Checklist*. At this point, the Student File becomes the responsibility of the Registration Manager and Office Support Team.

When the Enrollment and Registration forms have been completed following the New Student Orientation, they are downloaded and attached to the appropriate electronic Class File, in the sub-folder titled "Registration and Enrollment Documents." Completed Student Files are organized by enrollment year, and then alphabetically by last name.

Student Attendance, Academic Progress, and Performance Records

Student Attendance is recorded electronically via the mobile app version of the Student Portal. Students use the app to record their "Check In" time upon their arrival class, and their "Check Out" time upon departure from class. Written sign-in sheets, on which students must indicate their arrival and departure times, can also be used as back-up for residential (on-site) courses. Instructors, with backup from the SAP Compliance Team, are responsible for ensuring Students use the attendance app appropriately, or that physical *Class Attendance Sheets* are filled out completely and correctly.

To verify their presence and participation in the virtual classroom, students enrolled in IDL courses must also respond to Engagement Check questions, which are posted once per hour of each scheduled class session via Microsoft Forms in Microsoft Teams for Education. Each Engagement Check question is posted and available in the class team, on the channel where the active class session is being held, for 15 minutes only (e.g. Question 1 is available only from 7:00pm until 7:15pm; Question 2 is available only from 8:00pm until 8:15pm; and so on). Engagement Check questions are automated and cannot be retrieved once the scheduled window to answer is closed. Students are not required to answer the Engagement Check questions correctly, but they must provide an answer to each question in order to verify the attendance they are logging via the Student Portal app. Students who fail to respond to an Engagement Check question will not receive credit for attendance during the corresponding hour of class, regardless of whether they are "Checked In" during that time.

Data from the attendance app is monitored weekly and tracked in Lab Four's electronic Student Information System (SIS), which automatically calculates each student's current attendance rate, total hours attended, and minimum hours needed to regain compliance with the Attendance Policy if their attendance rate drops below the 80.00% threshold.

All graded assignments are submitted electronically via Moodle. Grades are then entered on the administrative side of the SIS on a weekly basis by SAP Office Support, which calculates each student's updated cumulative grade average.

All students are provided their updated grade point average and attendance rate via the Student Portal. Students whose grade point average falls below 70% or whose attendance rate falls below 80% after the SAP is updated each week also receive email communications from our SAP Compliance team, letting them know they are in violation of Lab Four's SAP and/or Attendance Policies and require corrective action.

Certificates of Completion and certification exam results are attached to the electronic class file at class close-out and attached to individual electronic files for each student. At the class close-out, final SAP and Attendance records are exported and attached to the electronic class file.

Employee Files

All New Hire Paperwork, per the *Employee File Checklist*, is to be completed as part of the onboarding process on or before each new employee's first day of work. Once all documents are completed, the file is audited by the Office Manager and the employee's information is entered into the payroll system as well as the Human Resources management software, HRWeb.

Once the employee's information has been entered into the payroll system and HRWeb, an Employee Binder is created for them. The Employee Binder will hold all of the employee's New Hire paperwork and includes designated spaces for later additions such as performance reviews, PTO requests, and professional development.