Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

General Description

The Master of Science degree in Cybersecurity Defense at the New England Institute of Technology is designed for technology professionals with experience in networking, cybersecurity or software engineering who desire to advance their leadership and cybersecurity skills as a precursor to a leadership role. From multi-national corporations to local small businesses, cybersecurity defense is an integral piece of an organization's strategy. Information and the technology infrastructure it resides on are two of an organization's most valuable assets and these are often continuously threatened or under active attack. Successful defense and protection of these assets requires a trained cybersecurity professional who not only understands the technical aspects, but also is aware of strategic business interests. An effective cybersecurity leader requires a blend of operational and technical expertise, leadership and management of projects and teams, and a solid foundation in the principles of cybersecurity.

The MSCD degree blends technical knowledge and essential cybersecurity skills with business management and enterprise leadership principles that drive organizations today. The program weaves technical topics such as penetration testing and digital forensics with project management, leadership and risk assessment.

While the bachelor's degree in Cybersecurity and Network Engineering prepares graduates to secure, design, and implement networks, databases and applications, the master's program provides graduates with the ability to analyze business scenarios and assess risk, anticipate and respond to a continuously changing environment, address post-incident business impacts and effectively assign resources to the entities that comprise the enterprise information systems.

The program emphasizes the relevance of continuous learning to personal and professional growth through the combination of advanced technical courses and an integrated management core. Employment opportunities may include positions such as Chief Information Security Officer (CISO), Project Manager, Incidence Response or Forensics Team Lead, Director of Software Security Engineering, Chief Information Officer (CIO), or Chief Technical Officer (CTO).

The MSCD program's mission is to prepare information technology professionals to be workplace and community leaders in cybersecurity, able to identify and assess cybersecurity vulnerabilities under their responsibility, to develop viable, actionable plans to address those vulnerabilities and to implement, monitor and respond in accordance with those plans. The mission and program are built around the components of the CISSP (Certified Information Systems Security Professional) Certification, which is often required for a cybersecurity professional to advance in the field and the requirements for an NSA Center for Academic Excellence in Cyber Defense (NSA CAE CD). The program is not directly designed to prepare graduates for certification, instead program and course objectives are closely aligned with the CISSP knowledge areas and CAE CD knowledge areas.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Program Mission

The NEIT Masters in Cybersecurity Defense seeks to prepare information technology professionals to be workplace and community leaders in cybersecurity, able to identify and assess cybersecurity vulnerabilities under their responsibility, to develop viable, actionable plans to address those vulnerabilities and to implement, monitor and respond in accordance with those plans.

Learning Outcomes

Graduates of this advanced degree program will be able to demonstrate each of the following learning outcomes:

1. Proficiency in identifying vulnerabilities, anticipating attacks, using monitoring tools, and developing defensive strategies.

2. Understand and analyze the technological, human, and policy challenges in this field through hands-on experience of cyber vulnerabilities, attacks, and defenses.

3. Create a principled, forward-looking framework to protect organizations against cyber threats and design organizational resilience, and crisis management and response capabilities.

4. Understand of cybersecurity and privacy through comprehensive consideration of technology and policy, including economic, human, legal, organizational, and socio-political factors.

5. Understand the security and privacy implications of emerging technologies, such as big data, cloud computing, mobile computing, social networks, the internet of things, and Web 2.0 applications.

6. Understand role of communication in leading teams and organizations, and develop communication skills necessary to influence and motivate teams.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Curriculum
Sample Plan of Study
Course Schedule subject to change.

Term I			C	L	T
Course No.		*Course Title*	C	L	T
IT	544	Cloud Computing	4	0	4
MGM	533	Advanced Project Management	4	0	4
			8	**0**	**8**

Term II			C	L	T
Course No.		*Course Title*	C	L	T
IT	524	Information Systems Security	4	0	4
MGM	514	Leadership	4	0	4
			8	**0**	**8**

Term III			C	L	T
Course No.		*Course Title*	C	L	T
CYB	536	Network and System Information Assurance	4	0	4
CYB	538	Security Auditing and Risk Management	4	0	4
		Optional			
CPT	591	Workplace Practicum I	0	20	1
			8	**0/20**	**8/9**

Term IV			C	L	T
Course No.		*Course Title*	C	L	T
CYB	542	Ethical Hacking in Defense of the Enterprise	4	0	4
CYB	552	Digital Forensic & Breach Investigations	4	0	4
		Optional			
CPT	592	Workplace Practicum II	0	20	1
			8	**0/20**	**8/9**

Term V			C	L	T
Course No.		*Course Title*	C	L	T
CYB	548	Robust Incident Response Planning	4	0	4
CYB	558	Secure Software Development	4	0	4
		Optional			
CPT	593	Workplace Practicum III	0	20	1
			8	**0/20**	**8/9**

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Term VI					
Course No.		*Course Title*	*C*	*L*	*T*
IT	556	Master's Project	5	0	5
		Optional			
CPT	594	Workplace Practicum IV	0	20	1
			5	**0/20**	**5/6**
Total Quarter Credit Hours = 45-49					

Legend

C = Number of lecture hours per week
L = Number of laboratory hours per week
T = Total Quarter Credit Hours where each lecture hour per week is one credit, every 2-4 laboratory hours are one credit depending on the expected amount of pre- or post-lab work.

Subject to change.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Degree Progress Checklist

Check off each completed course.

T1	IT	544	_____
	MGM	533	_____
T2	IT	524	_____
	MGM	514	_____
T3	CYB	536	_____
	CYB	538	_____
	Optional		
	CPT	591	_____
T4	CYB	542	_____
	CYB	552	_____
	Optional		
	CPT	592	_____
T5	CYB	548	_____
	CYB	558	_____
	Optional		
	CPT	593	_____
T6	IT	556	_____
	Optional		
	CPT	594	_____

Subject to change.
Please see your advisor for any questions.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Course Descriptions

CYB 536 Network and System Information Assurance
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
The security threats and risks that govern computer systems and networks can be mitigated by using a variety of security models, mechanisms and protocols. Such mechanisms are used to implement security policies that are defined in a risk management strategy. Designing security architecture is a critical task that includes securing hardware, software and networks. This course introduces security models and the concept of subjects and objects in order to discuss authorization and access control. Case studies of how authentication and access control are implemented in real-life systems are also presented. Security risks that are related to networks are equally important. Students define secure communication channels and present known and established network security protocols (SSH, SSL, IPSec, etc.). Special cases such as wireless and mobile networks are also examined to demonstrate how traditional security architectures can be adapted to facilitate different requirements.

CYB 538 Security Auditing and Risk Management
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
In this course, students appraise all standards and information technology (IT) security audit processes, evaluate security controls, and examine governance of compliance and control responsibilities. Most organizations are required to comply with IT security regulations and/or standards resulting from the establishment of the Sarbanes-Oxley Act, General Computing Controls, the Gramm–Leach–Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), and the Payment Card Industry Data Security Standard (PCI DSS) Students will become familiar with these standards and regulations.

CYB 542 Ethical Hacking in Defense of the Enterprise
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
An ethical hacker is a security expert who attacks a system on behalf of the system's owners. This course focuses on discovering network vulnerabilities that a malicious hacker can exploit. The course explores penetration testing, footprinting and social engineering, scanning and enumeration, operating system weaknesses, and the methods used to hack web servers and wireless networks. Students perform hands-on projects using state-of-art hacking tools and techniques after extensive planning.

CYB 548 Robust Incident Response Planning
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
This course provides students with the background and skills to manage information security incidents to minimize impact on business operations. Topics include detection, investigation, and response to different types of security incidents. Students explore these topics by developing incidence response plans; utilizing industry-standard processes and tools for investigating information security incidents; and recommending processes for incidence response that adhere to legal, regulatory, and organizational compliance. Students who have completed the course have a comprehensive view of cybersecurity incident detection and response.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

CYB 552 Digital Forensic & Breach Investigations
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
This course explores the expertise required to conduct digital forensic investigations. Topics include investigation methods, problem-solving techniques, current forensics analysis tools, digital evidence acquisition and control, and impact of ongoing technological changes on digital forensics. Student projects include scenario-based investigations in investigating cybersecurity breaches.

CYB 558 Secure Software Development
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
Software applications are often characterized as the cement of our times due to the high prevalence of computer systems in all aspects of our lives: banking, health, transportation, retail, even "smart home" systems. As a result, managing application security risks is a quite critical aspect of information security. This course aims to justify the importance of application security, firstly by analyzing how security can be integrated in the software development lifecycle. We demonstrate methods to identify vulnerabilities and discuss techniques that can be used to mitigate them and improve the overall security of software applications. Closely coupled with applications are databases that support them and facilitate data storage, retrieval and corresponding transactions. Concurrency control is a critical issue in database security. Methods for concurrency control and several aspects of database security, focusing on relational databases are discussed.

IT 524 Information Systems Security
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
Students in this course will get a high-level overview of the information security topics for which today's corporations need competencies. Essential security topics in this course cover network fundamentals and applications, standards, privilege management, environmental security issues, defense in depth, risk management, vulnerability assessments, business continuity planning, security policies, incident handling, web application security, and advanced persistent threats.

IT 544 Cloud Computing
4 Class Hours 4 Quarter Credit Hours
Pre/Co-requisite: MGM 533
This course provides students with a detailed exploration of the cloud-computing paradigm. After studying cloud architecture, students will study the strategic, risk and financial impact of utilizing this platform. Pertinent topics also include design, implementation and security aspects of applications stored in the cloud. The course will cover the entire spectrum of moving applications into the cloud.

IT 556 Master's Project
5 Class Hours 5 Quarter Credit Hours
This course is graded as pass/fail. Information Technology and Cybersecurity Defense students must choose one of the following two options:

Option 1: The capstone project requires IT and CD students to demonstrate their competence in the skills and knowledge associated with their degree program. It is designed to show the in-depth learning and higher-order thinking of students. With this option, students must choose a project in the field of information technology or cybersecurity and then plan, organize, implement, and work towards the completion of the project in a controlled manner, to meet the goals and objectives of their project. The capstone project is carried out by an individual student and may be derived from the student's workplace where the student can exploit the workplace experience to benefit both the student and the student's

Cybersecurity Defense
Master of Science Degree
*(For students entering their program
October 2019 – 202010 or later)*

place of employment. Before beginning work, each capstone project must first be approved by an Information Technology Faculty Advisor. At the end of the project, the student will prepare a Final Project Report and defend this work product before the Faculty Advisor and a panel of other assigned faculty members.

Option 2: The master's thesis requires students to carry out an investigation of technology or methodology in which the student has a strong interest. The topic of this investigation or research should be an extension or continuation of the topics covered in the MSIT or MSCD curriculum. The topic must first be approved by an Information Technology Faculty Advisor. The thesis option requires a presentation of the paper to the Faculty Advisor and a panel of assigned faculty members.

CPT 591 Workplace Practicum I
20 Field Hours 1 Quarter Credit Hour
Prerequisite: Requires successful completion of four courses in the master's program and approval of the Graduate Director or Department Chair
In this optional course, students will use knowledge gained through previous coursework in the master's program with planned and supervised work experiences in the public or private sector. The course allows students to enhance the practical skills necessary for success by being exposed to the reality of the world of work beyond the boundaries of the campus and enhancing their self-confidence and career direction. Students are required to provide bi-weekly status reports to the Graduate Director while enrolled in this course.

CPT 592 Workplace Practicum II
20 Field Hours 1 Quarter Credit Hour
Prerequisite: CPT 591
This course is a continuation of the Workplace Practicum begun in CPT 591.

CPT 593 Workplace Practicum III
20 Field Hours 1 Quarter Credit Hour
Prerequisite: CPT 592
This course is a continuation of the Workplace Practicum begun in CPT 591 and continued in CPT 592.

CPT 594 Workplace Practicum IV
20 Field Hours 1 Quarter Credit Hour
Prerequisite: CPT 593
This course is a continuation of the Workplace Practicum begun in CPT 591 and continued in CPT 593.

MGM 514 Leadership
4 Class Hours 4 Quarter Credit Hours
Leadership is about developing a vision and inspiring others to achieve that vision. It is wayfinding through effective communication. Leaders seek to understand and shape organizational culture, while effecting and supporting positive change. This course provides aspiring leaders with tools to develop a confident voice for their own current and future leadership roles. The major theories of leading and managing people and organizations will be applied to real leadership situations in organizations ranging from start-ups to large enterprises, as well as real leaders in the student's chosen field. While seeking a deep understanding of their own leadership style, students will examine the interaction between leadership and organizational culture, culminating in the development of a personalized comprehensive leadership development plan.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

MGM 533 Advanced Project Management
4 Class Hours 4 Quarter Credit Hours
Project management is more than merely parceling out work assignments to individuals and hoping that they will somehow accomplish a desired result. In fact, projects that could have been successful often fail because of such take-it- for-granted approaches. Individuals need hard information and real skills to work successfully in a project environment and to accomplish project objectives. Topics include project management life cycle and process; identifying and selecting projects; developing a project proposal; techniques for planning, scheduling, resource assignment, budgeting, and controlling project performance; project risks; project manager responsibilities and skills; project team development and effectiveness; project communication and documentation; and project management organizational structures. The concepts in the course support the project management knowledge areas of the Project Management Institute's A Guide to the Project Management Body of Knowledge (PMBOK® Guide).

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Questions & Answers

1. When and where do my classes meet?

If you choose the on-campus course option, your course will meet in the evening, once a week from 6:30-10 p.m. Classes will usually take place at the main campus in East Greenwich, RI.

At the beginning of each term you will receive a detailed schedule giving the exact time and location of all your classes. The university requires that all students be prepared to take classes and receive services at any of NEIT's locations where the appropriate classes and services are offered.

2. How large will my classes be?

The average size for a class is about 15 to 20 students; however, larger and smaller classes occur from time to time.

3. How long should it take me to complete my program?

To complete your degree requirements in the shortest possible time, you should take the courses outlined in the prescribed curriculum. For a typical six-term curriculum, a student may complete the requirements in as little as 18 months.

4. How long is each academic term?

Courses at New England Tech are 10 weeks long, with four terms offered per year, starting in January, April, July, and October.

5. Is NEIT accredited?

NEIT is accredited by the New England Commission of Higher Education (formerly the Commission on Institutions of Higher Education of the New England Association of Schools and Colleges, Inc.). Accreditation by NECHE is recognized by the federal government and entitles NEIT to participate in federal financial aid programs. Some academic departments have specialized professional accreditations in addition to accreditation by NECHE. For more information on accreditation, see NEIT's catalog.

6. Can I transfer the credits that I earn at NEIT to another college?

The transferability of a course is always up to the institution to which the student is transferring. Students interested in the transferability of their credits should contact the Office of Teaching and Learning for further information.

7. Can I transfer credits earned at another college to NEIT?

Transfer credit for appropriate courses taken at accredited institutions will be considered for courses in which the student has earned a "B" or above. An official transcript from the other institution must be received before the end of the first week of the term for transfer credit to be granted for courses to be taken during that term. Students may transfer no more than 4 credits (one course).

8. How many credits do I need to acquire my Financial Aid?

Students entering the program will be eligible for various forms of financial aid, including loans, if they take at least 4 credits per term.

9. What does my program cost?

The cost of your program will be as outlined in your enrollment agreement, along with your cost for books and other course materials.

10. What kind of employment assistance does NEIT offer?

The Career Services Office assists NEIT students and graduates in all aspects of the job search, including resume writing, interviewing skills, and developing of a job search strategy. Upon completion of their program, graduates may submit a resume to the Career Services Office to be circulated to

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

employers for employment opportunities in their fields. Employers regularly contact us about our graduates. In addition, our Career Services Office contacts employers to develop job leads. A strong relationship with employers exists as a result of our training students to meet the needs of industry for over fifty years. No school can, and NEIT does not, guarantee to its graduates employment or a specific starting salary.

11. Where will job opportunities exist?
Graduates have obtained employment in the local area. However, one of the exciting aspects of NEIT's programs is the ability to look nationally for employment opportunities. Graduates will have the depth of confidence and the technical and managerial education to successfully lead in the IT industry, both now and well into the future. Successful graduates may be able to advance their careers by qualifying for positions such as Project Manager, Network Manager, Chief Information officer (CIO), Chief Technical Officer (CTO), Business Analyst or Systems integrator.

12. Do I need a cybersecurity, computer science or information technology degree to enter the program?
Yes. A B.S. degree in computer science, information technology or a related field from an accredited institution is required for before beginning this degree program. You may enroll in this program pending the completion of your current B.S. degree. Significant professional experience may be considered in lieu of an appropriate degree. A transcript and/or a resume should be supplied to satisfy either of these requirements.

13. Do I need a certain grade point average to enter the program?
Yes, you will need a 2.5 grade point average to enter the program.

14. Are there any other special entrance requirements?
Yes. You will need to write a personal statement as part of your admission process that details your interest in the program and how it will enable you to accomplish your professional goals.

15. Do I need to maintain a certain grade point average?
Yes. You are required to maintain a cumulative grade point average of at least 3.0 throughout the program. The minimum passing grade for a course in the MSCD program is a C (73%).

16. What happens if I earn less than a C in a course?
Students who earn less than a C in any course will be required to re-take the course the next time it is offered. If the student does not earn a C or better in a course after the second attempt, he/she will be dismissed from the MSCD program. Students will only be allowed to re-take two courses.

17. For whom is this program designed?
The New England Tech Master of Science in Cybersecurity Defense is designed to prepare IT professionals for advancement into management and senior management roles. The program builds essential knowledge of technical themes in enterprise IT, while also providing the core business administration, management and leadership skills that IT managers need.

18. Will all or some of my classes be online?
You will have the opportunity to choose courses that are online or on-campus. You can mix them up any way you like to create a schedule that works for you and fits into your personal and professional life. The entire program can be completed completely online, though on-campus options exist for most courses as well.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

19. How do online courses work?

Online courses at New England Tech are crafted by a faculty-led team of learning and technology design experts to be interesting, relevant and engaging, and to have real impact on students in their lives and on their careers. They are not self-paced courses – you will have coursework to do every week and it is important to keep up.

You can do your coursework at any time of day. At times, there may be synchronous online meetings, but these will not happen often. You will be learning as part of a connected community that provides support, challenges your thinking, and reminds you that you are not alone. Instructors are present in the course and work with students to help them be successful. See Online Learning at NEIT for more information about online courses in the MSIT program.

20. What are the hardware and software requirements for the program?

	Recommended Minimum
Operating System:	Windows 10 or Macintosh OS X (10.14)
Processor:	2+ GHz
Memory:	4GB
Plug-ins:	Adobe PDF Reader, Flash Adobe PDF Reader, Flash and others as required by specific courses
Players:	QuickTime, Java Player, Java
Browser:	Chrome, IE, Safari, Edge, Firefox (all latest versions)
Display:	1024x768
Software:	Office 365 (2016)
Internet Connection:	FiOS/DSL/CABLE DSL/CABLE
Email Account:	New England Tech student email account
Sound Card:	Required
Other (some programs):	• A webcam (the one built into your laptop or iPad should be fine) • A microphone (built into the computer or headset is handy). • A digital camera (the one on a smart phone is fine).

Online students must be capable of installing and maintaining their own computer's hardware and software. New England Tech does not assist students with the setup of their computers.

Information about obtaining the software (if any) will be made available to you at the start of each course.

Note: Tablets and smartphones can be convenient for reading course materials and email but will not be sufficient for doing all of your course work.

21. I'm not so sure about online courses. What do I need to do to be successful?

No special equipment is required – just a modern Windows or Mac computer, an office suite such as Microsoft Office, and a broadband Internet connection. A webcam and microphone may be required for some activities.

New England Tech Online courses help acclimate you to the technology and build your skills and your confidence as you go. We provide 24x7 support via phone, email or chat to help you with computer or online system issues. Tablet computers can be useful for doing course readings, watching course videos,

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

and catching up on course discussions; but a tablet will not be sufficient for doing all your coursework – be sure you have regular access to a laptop or desktop computer.

Most importantly, you'll need to set aside time to do your coursework. This program is challenging. In an online course, you should expect to spend as much time as you'd spend in the classroom for an on-campus course, plus time for reading, projects, group work and other assignments.

22. What makes New England Tech's MS Cybersecurity Defense program different from others?

- The program has a carefully crafted blend of advanced technical education with leadership and management skills. The curriculum balances crucial enterprise cybersecurity knowledge with mastery of business and management skills preparing you to be a cybersecurity leader in your organization.
- Courses are taught by professional practitioners and leaders in the field with advanced certifications (PMP, CISSP, etc.) who bring real life examples into the classroom.
- The program builds on technical knowledge students already possess so that graduates are comfortable in many of an organization's technical leadership roles. Graduates are ready for roles as Project Manager, Chief Information Officer (CIO), Chief Technical Officer (CTO) or Chief Information Security Officer (CISO).
- Courses are focused on practical, real-world scenarios to convey the skills and concepts.
- Our curriculum builds a long-term, adaptable base of leadership skills to fuel your career advancement.
- A curriculum based on the CISSP certification (Certified Information Systems Security Professional)
- Program moving towards NSA Center of Academic Excellence in Cybersecurity Defense.
- Ten-week long courses keep you focused and are easier to digest, and enable you to finish your Master's degree in as little as 18 months.
- Ability to take the courses in the classroom or online (most cybersecurity programs are online only)
- A rich virtual environment (SkyTap) for simulations and practical exercises.
- Graduates are given the tools to make decisions that support the strategic goals of the organization.
- 24x7 technical support by email, chat or phone helps you work on your schedule.

23. What are the admissions requirements to the Master's program?

A bachelor's degree from an accredited institution, with a minimum GPA of 2.5, is required for admission to this degree program. You may enroll in this program pending the completion of your current bachelor's degree. Successful applicants will typically have a B.S. degree in computer science, information technology or a related field, or have considerable professional experience in IT. A transcript and/or a resume should be supplied to satisfy either of these requirements.

You'll also provide a Personal Statement as part of your admission process – a brief essay that details your qualifications and interest in the program and how it will enable you to accomplish your professional goals.

Cybersecurity Defense
Master of Science Degree
(For students entering their program
October 2019 – 202010 or later)

Technical Standards
These technical standards set forth by the IT department establish the essential qualifications considered necessary for students admitted to the program. The successful student must possess the following skills and abilities or be able to demonstrate they can complete the requirements of the program with or without reasonable accommodation, using some other combination of skills and abilities.

Cognitive Ability
- Good reasoning and critical thinking skills.
- Ability to learn, remember and recall detailed information and to use it for problem solving.
- Ability to deal with materials and problems such as organizing or reorganizing information.
- Ability to use abstractions in specific concrete situations.
- Ability to separate complex information into its component parts.
- Ability to perform tasks by observing demonstrations.
- Ability to perform tasks by following written instructions.
- Ability to perform tasks following verbal instructions.
- Possession of basic keyboarding skills and knowledge of computer programs.

Communications Skills
- Ability to speak in understandable English in a classroom situation on a one-on-one basis as well as before a group.
- Ability to communicate effectively with faculty and other students.
- Ability to demonstrate and use the knowledge acquired during the classroom training process.
- Ability to verbally express technical concepts clearly and distinctly.
- Ability to express thoughts clearly.
- Adaptive Ability
- Ability to remain calm in the face of computer lab equipment and/or software failure.
- Ability to maintain emotional stability and the maturity necessary to interact with members of the faculty and students in a responsible manner.
- Ability to tolerate the differences in all students, faculty, and administration.
- Ability to follow instructions and complete tasks under stressful and demanding conditions. Ability to adapt in a positive manner to new and changing situations with an open mind and flexibility.
- Ability to think clearly and act quickly and appropriately in stressful situations.

Physical Ability
- Ability to sit continuously at a personal computer for long periods of time in order to learn and become proficient in computer programming and networking.
- Ability to perform learned skills independently, with accuracy and completeness within reasonable time frames in accordance with classroom and business procedures.
- Manual Ability
- Sufficient motor function and sensory abilities to participate effectively in the classroom laboratory.
- Sufficient manual dexterity and motor coordination to coordinate hands, eyes and fingers in the operation of computers and business equipment.

Sensory Ability
Visual
Acute enough to see clearly and interpret the contents on the computer screen.