



SCHOOL CATALOG

2023-2024

Virginia Institute of Science & Technology

2070 Chain Bridge Road, Suite G100
Vienna, VA 22182

Tel: 703-880-8446
Fax: 703-880-8728
www.VISTedu.us

VIST is accredited by Accrediting Commission of Career Schools and Colleges (ACCSC)

VIST is approved to offer GI Bill® educational benefit by the Virginia State Approving Agency.

VIST is certified to operate by the State Council of Higher Education for Virginia (SCHEV)

Rev. November 9, 2023

VIST is located on the 1st floor of the building pictured above in suite G100.

★★★ Disclaimer ★★★

This catalog serves as an official document of the Virginia Institute of Science & Technology (“VIST”). It provides general information about VIST’s degree programs, admission requirements, course offerings, policies, procedures, regulations that govern the school during the 2023-2024 academic year.

This school catalog is current at the time of publishing with the effective dates stated below. At any time, it may be necessary or desirable for VIST to make changes to this catalog due to the requirements and standards of the School’s accrediting body, state, licensing agency, U.S. Department of Education, market conditions, employer needs, or other reasons. The school reserves the right to make changes to any portion of this catalog, including the amount of tuition and fees, academic programs and courses, program completion and graduation requirements, policies and procedures, faculty and administrative staff, the academic calendar, attendance policies, grievance and complaint procedures, and other provisions.

Tuition and fees are reviewed annually; tuition changes do not occur mid-term; changes to tuition are communicated at least two terms in advance.

VIST also reserves the right to make changes in equipment and instructional materials; modify curriculum; and, when size and curriculum permit, to combine courses. The president should be contacted for information concerning any such changes. These changes are inserted into the catalog as an addendum and will be available on the VIST website at www.VISTedu.us.

Compliance with the policies, procedures, and regulations set forth in this catalog is the personal responsibility of each student.

This Catalog supersedes and replaces all previously published versions and is made available to students on the VIST website at www.VISTedu.us.

VIST is a non-discriminatory institution when admitting students to all programs, and it is an equal opportunity employer.

Effective: Fall 2023 thru the end of Summer 2024 Quarters

© 2023 ❖ VIST

Table of Contents

1. General Information.....	6
About VIST	6
School History	6
Mission Statement	7
Instructional Philosophy	8
Core Values	8
Legal Control and Ownership	8
Advisory Expert Board (AEB).....	9
Selected Faculty at VIST.....	9
Non-Discrimination Policy.....	10
VIST Facilities and Equipment	10
Library	12
Operation Hours	13
2. Admission Information	14
Programs Offered in 2023-24 Academic Year.....	14
Admission Requirements	14
Admissions Procedure	15
Enrollment Agreement	16
Transfer Students & Transfer Credit	16
Course Matching or Substitution.....	16
Academic Calendar for 2023-2024	16
Holidays.....	17
Campus Security Act Information.....	17
Faculty Advising & Office Hours	17
General Policy for G.I. Bill Beneficiary.....	17
3. Tuition, Fees & Scholarships.....	19
Tuition and Fees	19
Other Fees.....	19
Cancellation & Tuition Refund Policy	19
Late Payment Fee	21
VIST Scholarship	21
4. Academic Policies	22
Quarter and Credit System	22
Calculation of Credit	22
Grade Point Average (GPA).....	23
Graduation Requirement	23

Satisfactory Academic Progress (SAP) Policy.....	23
Effects of Incomplete “I” Grade on SAP	25
Effects of Repeat Course “R” on SAP	25
Effects of Transfer Credits “TC” on SAP	25
Effects of Withdrawals “W” on SAP	26
Academic Warning.....	26
Academic Probation	26
Academic Dismissal	27
Reinstatement as a Regular Student	27
Attendance Policy.....	28
Grade Appeal Policy	28
5. Student’s Rights and Responsibilities	29
Freedom of Access	29
Sexual Harassment Policy	29
Formal Grievance Procedure.....	29
Civil Rights Compliance	31
Catalog of Record.....	31
Privacy of Student Records	31
Retention of Student Records.....	31
Non-Discrimination Policy.....	31
Copyright Law.....	31
Student’s Code of Conduct.....	32
Statement of Academic Freedom	33
Transferability of VIST Credits	33
Credit for Prior Learning.....	33
Academic Honesty Statement of Policy.....	33
Drugs and Alcohol Policy	34
6. Descriptions of Academic Programs	35
MS in Cybersecurity & Information Assurance (MSCIA)	35
MSCIA Program Objectives (PO).....	35
Core Courses	36
Specialization Areas.....	36
Electives	36
Capstone.....	37
7. Student Services.....	38
Academic Advising.....	38
Career Services Center	38
Social Adjustment and Coping Skills.....	39

New Student Orientation	39
Student Resources	39
Library and Learning Resources System (LRS).....	39
Curricular Practical Training (CPT).....	39
Mental Health and Suicide Prevention Lifeline	41
8. Course Descriptions.....	42
Academic Courses.....	42

1. General Information

About VIST

VIST is a private school established in the Commonwealth of Virginia. The VIST campus is located in Vienna, Virginia at 2070 Chain Bridge Rd, Suite G100, Vienna, Virginia 22182-2500. Vienna is a suburb of the nation's capital, Washington D.C. It is located within a 25-40-minute drive of most of the Greater Washington Metropolitan area (inclusive of Southern Maryland, Washington, D.C., and Northern Virginia). The VIST campus is conveniently situated within walking distance of both the Greensboro and Spring Hill stations of the silver line of the Washington, D.C. Metro rail system.

VIST's official Contact info is: Tel: +1-703-880-8446, Fax: +1-703-880-8728, and contact email: info@VUST.us.



VIST Campus Building-Suite G100

School History

In 2009, Dr. Martin Ma and his partners first formed an initiative committee for the purpose of establishing a new, private institute in Northern Virginia. The committee members engaged expert consultants to conduct marketing analysis, feasibility study, and risk assessment profile for the creation of the new institute while at the same time engaging in a fundraising campaign to bring interested investors into the project. VIST was formally incorporated in the Commonwealth of Virginia in January of 2013. By March of 2015, the board of directors had secured a permanent campus home for VIST in McLean, Virginia, equipped with classrooms, offices, labs, a library, and other facilities.

In May 2016, The State Council of Higher Education for Virginia (SCHEV) certified Virginia Institute of Science & Technology to operate in the Commonwealth of Virginia. On September 16, 2016, The Virginia Institute of Science & Technology had its grand opening ceremony. 2006 Nobel Prize in Physics Laureate Honorable Dr. Mather is Keynote Speaker at the ceremony. The institute was also proud that honorable Amata Coleman Radewagen, U.S. Representative, was the speaker in the VIST Open Ceremony. The former Assistant Speaker of the US House of Representatives, US Senator, honorable Chris Van Hollen, and US Senator honorable Ben Cardin gave video greetings. US Congressman

honorable John Delaney granted the Certificate of Special Congressional Recognition to Virginia Institute of Science & Technology. US Senator honorable Tim Kaine, honorable US House Representatives Barbara Comstock, Gary Connelly, Donald Payne, Jr, and Virginia Lt. Governor honorable Ralph Northam assigned their representatives to attend the VIST Open Ceremony to present Official Citations and Greeting letters to VIST. Former Chief Finance Officer of US Department of labor Samuel Mok, Maryland Senator Susan Lee, Virginia Delegate and Majority Leader Tim Hugo, Directors of Information Technology from US Department of Labor and US Office of Personnel Management (OPM), as well Fairfax County leaders and many community leaders attended the VIST open Ceremony.

In Fall 2016, the first group of 17 students was admitted in the program of Master of Science in Cybersecurity and Information Assurance (MSCIA) at VIST. Many of them were senior technical leaders in their organizations or governmental agencies.

June 9th, 2018, was a historic day for VIST because the first Commencement Ceremony was held in Tysons Campus. The first group of 17 students successfully completed their Master's program of Cybersecurity & Information Assurance (MSCIA) and received their Master of Science (MS) degrees.

On November 1st 2023, VIST became accredited by Accrediting Commission of Career Schools and Colleges (ACCSC)

VIST first Commencement Ceremony.



Mission Statement

The mission of VIST is to prepare students for rewarding careers through quality educational programs that meet the changing needs of employers and the community. In order to fulfill this mission, VIST offers a Master's degree in Cybersecurity and graduate certificates in related fields.

To meet the needs of a diverse community of learners, VIST provides education that balances technical, professional, and critical thinking components. In pursuit of this mission, the Institute seeks to provide:

- A quality learning experience by employing faculty committed to learning and who demonstrate effective teaching skills
- Relevant curricula through input from the governing board, advisory boards, and graduates
- Student success through a comprehensive support program including financial planning, academic assistance, and other student services

Instructional Philosophy

VIST believes in a student-centered approach. We seek to maximize students' personal and academic growth while providing relevant skills and knowledge leading to satisfying careers. The Institute is able to achieve these goals through carefully planned academic programs and career advising, including timely curriculum revisions, hands-on learning experiences, and individualized assistance.

Instructional Focus: Programs are directed toward specific instructional goals coupled with small class sizes. All curricula, presentations, supportive reference materials, and student-teacher interactions are collectively driven by this strategy.

Communication: Effective use of communication reinforces the instructional message. Creative seating arrangements and small group projects are used to encourage student to student and student to faculty interaction. Programs are structured to cultivate an environment of teamwork.

Self-Discovery: Hands-on learning using actual equipment is essential to the Institute's instructional methodology. The Institute recognizes hands-on learning as a key to long-term retention of information. In the final analysis, the Institute combines sound instructional technology with an insight into the career market to produce a valuable and unique educational experience.

Core Values

The core values we uphold at VIST are:

- 1. Diversity:** VIST welcomes students from all over the world and fosters equal participation of all its constituents.
- 2. Lifelong Learning:** VIST stimulates and promotes learning and life-long knowledge retention through continuing education.
- 3. Affirmative Spirit:** VIST promotes integrity and harmonious work with pride and compassion.
- 4. Partnership:** VIST cooperates with all its stakeholders, including students, faculty, staff, and community citizens.

Legal Control and Ownership

VIST is an independent institution governed by a self-perpetuating Board of Directors (BOD) who have the ultimate fiduciary responsibility for VIST, its finances, its human resource policies, its ethical and honest behavior, and its commitment to equal opportunity regardless of race, color, religion, national origin, age, political views, physical disabilities, or sexual orientation.

The Chairman of the Board of Directors (BOD) is appointed by the Board and has the authority to carry out the decisions of the Board, to maintain open communication among Board members, and to serve as the direct supervisor of the VIST President.

The President is the Chief Executive Officer of VIST and is responsible to the Board of Directors through its Chairman. The President has the authority and responsibility to manage the affairs of the institution in such a manner that ensures the VIST mission is pursued and its vision advanced. The Chairman shall be responsible for annual evaluations of the President and for seeking input from Board members and other key constituencies.

The primary function of VIST is teaching and learning, and VIST's faculty are recognized and rewarded for good teaching and mentoring. VIST instructors are also expected to be active practitioners within their professional fields and to be adept at developing student engagement in real-life job situations.

The control of School's operations rests with its Board of Trustees, which is composed of the following members:

BOD Members:

- Chairman & CEO: Dr. Martin Ma
- Secretary & Director: Dr. Mary Ma
- Trustee: Dr. Doris Sartor
- Trustee: Mr. Renzeng Zhang
- Trustee: Dr. William Chang
- Trustee: Dr. Jim Chen

Advisory Expert Board (AEB)

The Advisory Expert Board (AEB) is a group of volunteer experts in their field who serve as advisors to the President at VIST.

The EAB members consist of external experts who are Presidents, VPs, Deans, and professors in accredited American universities or well-known international universities, senior faculty at VIST, and student representatives (nonvoting delegates). They are committed to helping VIST maintain a standard of excellence in education.

Key EAB members:

- The Co-Chair of AEB is Dr. Jim Chen. Dr. Chen is full professor of Computer Science at George Mason University (GMU). He is currently director of the Computer Graphics Lab at GMU and associate editor-in-chief (EIC) of AIP/IEEE Computing in Science & Engineering (CiSE). He served as general co-chair of IEEE VR2006, program co-chair for IEEE VR (2002, 2003, and 2004), and guest editors for IEEE Computational Science & Engineering, CiSE, and PRESENCE. Jim's research interests include computer graphics, virtual reality, visualization, networking, and simulation. He authored 2 books, edited 2 conference proceedings, published over 80 research papers, and acquired 3 patents. Jim guided 11 Ph.D. dissertations. Six of his former Ph.D. students are currently professors. Jim received honorary professorships at Fudan University, Southwest Jiaotong University, Beijing Jiaotong University, Hoseo University, Sichuan Normal University, and Xihua University.
- Dr. Doris Sartor, AEB member, Ed.D. in Education, Auburn University
- Dr. Harry Wechsler, AEB member, Ph.D. in Computing Engineering, University of California, Irvine. Full Professor at George Mason University for more than 35 years.

Selected Faculty at VIST

- Dr. Yuan (John) Jiang, Ph.D. in Electrical & Computing Engineering, Columbia University, 1991
- Dr. Harry Wechsler, Ph.D. in Computing Engineering, University of California, Irvine, 1975
- Dr. George Zhang, Ph.D. in Electrical & Computing Engineering, University of Utah, 1994
- Dr. Jim Chen, Ph.D. in Computer Science, University of Central Florida, 1995
- Dr. Martin Ma, Ph.D. in GIS & Remote Sensing, University of Oklahoma, 1993
- Dr. Paul Wang, Ph. D. in Computer Science, George Mason University, 2004
- Dr. Sean Wang, Ph. D. in Computer Science, George Mason University, 2003
- Dr. Xiaoliang (Leon) Zhao, Ph.D. in Computer Science, North Carolina State University, 2002
- Dr. Doris Sartor, Ed.D. in Counseling & Psychology, Auburn University, 1992
- Dr. Jiuyi (Joe) Hua, Ph.D. in Transportation Engineering with emphasis on Computing Artificial Intelligence, University of Delaware, 1995

Non-Discrimination Policy

In accordance with Title IV of the Civil Rights Act of 1964, Title IX of Educational Amendments of 1972, Section 5 of the Rehabilitation Act of 1973, and Age Discrimination Act of 1975, VIST admits all qualified applicants regardless of age, sexual preference, gender, marital status, religion, national origin, creed, mental limitation, disability, or ethnic origin. VIST recruits and admits those students who have the potential to successfully complete their educational programs. The prospective student's motivation and interest in succeeding in his/her chosen field of study are important factors for admission consideration as well as the student's academic background and qualifications.

VIST Facilities and Equipment

The VIST campus is located in Vienna, Virginia, at 2070 Chain Bridge Road, Suite G100, Vienna, VA 22182. Our facility consists of the following: Classrooms, Teleconference Center/Conference Room, Laboratories, Cybersecurity Lab, System and Networking Lab, and Bigdata & VR Lab, Library with Online Library Capability, Faculty Offices, Student Study Rooms, Student Lounge area. Our classrooms are equipped with all-in-one Smart Touchscreen PC Desktop Computers, laptop computers, powerful servers, CISCO professional routers/switches/hubs/firewalls, high-speed Wi-Fi covering entire campus, 90"- Smartboard & projector, smart TVs (4). Microsoft Office 2018, and Adobe Professional software are installed in all the computers. The maximum number of students in classrooms is 25 and in the labs is 16.



VIST Classroom



Interactive Smartboard in Classroom



Conference Room & Distance Learning Center



Cybersecurity Lab

Library

The library contains an up-to-date collection of books, periodicals, newspapers, and other instructional materials that are readily accessible to all VIST faculty and students. The library also boasts touchscreen computers that allow faculty and students to access VIST's Online Library. The Online Library is accessible to each student and faculty member via their Populi account. The online Library contains thousands of periodicals and books in electronic format. In addition, students have access to the librarians to assist with information search needs. Access to the Librarian is also provided via Populi.

Online librarians are available daily (except holidays) based on the following schedule:

Monday - Friday 8AM to 10PM

Saturday - Sunday 12PM to 7PM



VIST On-Campus Library

Operation Hours

VIST Administration Office hours:

Monday – Friday: 9:00 a.m. to 6:00 p.m.
Saturday: 9:00 a.m. to 5:00 p.m.
Sunday: Closed

VIST Class hours:

Tuesdays - Friday: 2:00 p.m. to 6 p.m. or
5:30 p.m. to 9:30 p.m.
Saturdays: 9:00 a.m. to 1:00 p.m.
1:30 p.m. to 5:30 p.m.

2. Admission Information

Programs Offered in 2023-24 Academic Year

Our mission is to provide graduate programs in the area of cybersecurity in various industries.

During the 2023-24 academic year, we offer a Master of Science Degree in Cybersecurity & Information Assurance (MSCIA) program. Courses in this 54-credit program have been designed by cybersecurity academic and industry professionals to prepare graduates with job-ready skills. The program includes a choice of two specialization tracks: System Cybersecurity and Operation Assurance.

Consistent with the mission, purpose, and goals of the institutions, VIST offers the following programs.

Name of the Program	Credential Awarded	Graduation Requirements
Master of Science in Cybersecurity & Information Assurance (MSCIA) Specializations: <ol style="list-style-type: none"> a. Cybersecurity Systems b. Operation Assurance 	MS	54 Quarter Credit Hours

Admission Requirements

All applicants for admission to VIST must submit the required documents:

#	Domestic Admission Requirements	Programs
		MS in CIA
1	Application form (fee \$75)	<input type="checkbox"/>
2	Previous Degree	Bachelor's Degree*
3	Transcripts	<input type="checkbox"/>
4	Updated Resumé / CV	<input type="checkbox"/>

Students using the VA Education benefit program are also required to provide all transcripts from postsecondary training and military experience (if applicable).

#	International Admission Requirements	Programs
		MS in CIA
1	Application form (fee \$75)	<input type="checkbox"/>
2	Previous Degree	Bachelor's Degree*
3	Transcripts	<input type="checkbox"/>
4	Updated Resumé / CV	<input type="checkbox"/>
5	English Proficiency	<input type="checkbox"/>
6	Financial Documents**	<input type="checkbox"/>
7	Copy of Passport	<input type="checkbox"/>

* International degrees must be evaluated for the U.S. equivalency by a recognized agency.

** bank statement(s) showing that the international student has adequate funds available to cover the cost of one (1) academic year of study in the USA.

1. **Evidence of English Proficiency for International Students:** Any test score submitted must not be older than 2 years. This may include a minimum:

- TOEFL score of 61 (iBT) Or,
 - IELTS score of 5.0 Or,
 - iTEP score of 3.5 Or,
 - PTE score of 50 Or,
 - WAEC score of C6 or higher.
 - Duolingo score 90 or higher
 - Chinese College English Certification level 4 and above
2. **For transfer-in students:** Copy of passport, the I-94, and previous I-20 forms are required at the time of application. Please note: International students transferring from other US Universities, in addition to the current I-20, must also provide a copy of a bank statement(s) to verify sufficient funds.
3. **U.S. Equivalency:** Transcript for a degree earned outside of the U.S must be evaluated by a member of the Association of International Credentials Evaluators (AICE) **or** American Association of Collegiate Registrars and Admissions Officers (AACRAO) **or** the National Association of Credential Evaluation Services (NACES) or by any other authorized U.S based agency. (VIST does an initial pre-evaluation of foreign transcripts in the admissions process; however, to register and enroll in the program, an official third party transcript evaluation is required.)

Note: For a transfer student, who was admitted by any accredited degree granting institution in the U.S.A., VIST does not require foreign credential evaluation as a part of the admission process. *Furthermore, in cases, where a student's I-20 states that he/she has met the English Proficiency requirement, VIST will accept the previous school's language assessment and allow the student to register without taking one of the English Proficiency tests.

All required documents must be directly emailed to admission@VIST.us or mailed to:

2070 Chain Bridge Rd. Suite G100, Vienna, VA 22182.

Distance Education

Students desiring to take online courses are required to take Distance Education Readiness Survey. The survey measures students' ability to operate in an online platform environment.

The following are VIST's expectations from online students:

- Reliable internet access
- Modern computer or mobile device
- Camera and speakers for using the zoom platform

Admissions Procedure

The admissions process starts with a prospective student submitting an online application on the VIST's website. Then, the admissions office will contact the applicant to answer any questions and further explain the programs offered by VIST. The student will be requested to submit all required documents for enrollment. All admissions application documents can be submitted either in person, electronically, or by mail.

Notification of Admission: Notification of admission varies, but, in general, from the date the admission application is complete, it can take about a week for a decision to be made. Acceptance letters and other information will be sent via email to the applicants by the Admissions Department.

Pending Applications: Students who are making progress completing their application process and simply lacking documents or have files with incomplete information are classified as "pending" students. No acceptance letters may be sent to pending students until their file is complete.

Rejected Applications: Students who do not meet minimum admission standards will not be accepted into VIST. Students in this category will be notified of their denial of acceptance.

Enrollment Agreement

A student admitted to the Institute's program is not officially enrolled in the program until after the student has signed the Enrollment Agreement and completed registration for the first term with the required tuition and fees paid. A copy of the signed Enrollment Agreement is provided to the student once it is completed.

Transfer Students & Transfer Credit

Transfer students must meet the admission requirements in effect at the time of matriculation and must comply with the same admission procedures for each selected educational program as mentioned above. A transfer course will be labeled as TC in the student's transcript.

TC can be awarded for courses with a letter grade only "B" or above for graduate courses. Courses that are of a technical nature must have been completed within a recent time period (less than 7 years) to be considered for a TC award. Applicable courses taken for credit at international/foreign institutions must be evaluated by an approved Credential Evaluation Agency before a TC award can be considered. VIST will not accept credits from non-accredited US colleges and universities.

Per SCHEV regulation 8VAC40-31-140-B6, for all undergraduate programs, including certificate programs, a maximum number of transfer credits accepted cannot exceed 70% of the program completion requirement.

Transfer-out Policy for International Students:

1. All new international students are expected to complete at least two academic terms at VIST before transferring from the Institute. (Many US-based universities have similar policies; however, they operate on a semester-based system that is typically 15-16 weeks long. VIST offers classes on a 10-week term schedule. Therefore, two academic terms equal to 20 weeks of study.)
2. Students who would like to transfer out after completing two academic terms at VIST, will have to pay \$250 transferring/withdrawal fee.
3. A complete transfer-out form along with an acceptance letter must be submitted to DSO at least two (2) weeks before the new term begins. If a student misses this deadline, they must complete the upcoming term.

We encourage veterans to submit their Joint Service Transcript for evaluation.

Course Matching or Substitution

Every course considered for transfer will be examined for compatibility to a course offered for the same program at VIST with respect to the following, but not limited to:

- a. Course title, course description, and the number of credit hours, and/or
- b. In extenuating cases, if and when the condition in (a) above is not satisfied, the Director of Education could approve a course matching by considering the degree of similarity in content and learning objectives of the courses.

Academic Calendar for 2023-2024

VIST operates on a quarter system where each academic year is divided into four quarters: Fall, Winter, Spring, and Summer. Students may apply for acceptance into any one of these quarters.

Quarters	First Day of Classes	Last Day of Classes
Fall 2023	Oct 9, Mon	Dec 16, Sat
Winter 2024	Jan 8, Mon	March 16, Sat
Spring 2024	April 8, Mon	June 15, Sat
Summer 2024	July 8, Mon	Sept 14, Sat

Holidays

During the 2023-24 Academic Year, VIST will observe the following holidays, on which days there will be no classes, and our administrative offices will be closed:

1. New Year's Day (observed January 1st)
2. Martin Luther King Day (the third Monday in January)
3. Memorial Day (the last Monday in May)
4. Juneteenth Day (June 19th)
5. Independence Day (July 4th)
6. Labor Day (the first Monday in September)
7. Veterans Day (November 11th)
8. Thanksgiving Day (the fourth Thursday in November)
9. Christmas Day (observed December 25th)
10. Two (2) additional days between Dec 25 and Dec 31.

Conversely, the VIST does not observe the following holidays, on which classes are held:

1. Presidents Day (the third Monday in February)
2. Columbus Day (the second Monday in October)

Campus Security Act Information

VIST is located in a safe, suburban environment. Nevertheless, students are urged to take appropriate precautions to remain safe and to avoid potentially problematic situations. Students are to report all known or suspected crimes that occur on campus to the President. In a written report, students are asked to include the following information: the name of the person reporting the crime, the nature of the crime, the time and place of its occurrence, and the victim(s), if any, of the crime. Information regarding crimes in the area surrounding VIST's campus is available through the General Counsel. All crimes involving students are to be reported to the General Counsel as well as to the Fairfax County Police Department. A detailed Emergency Preparedness plan can be found on school's website at: vustedu.us

Faculty Advising & Office Hours

The faculty must be available to students at times other than scheduled classes. This availability (traditionally known as "office hours") can be provided in several ways, including but not limited to face-to-face office hours, asynchronous e-mail, synchronous online meetings, and/or phone/voice calls. The times, locations, and contact information about each faculty office's availability is posted in the specific course syllabus.

With the awareness that students may have problems that are handled best synchronously and/or face-to-face, faculty members will also make provision for meeting with students by appointment at a mutually convenient time if a student cannot meet during the stated schedule of availability. If for any reason, a faculty member cannot be available during the scheduled times, the faculty member will inform the administrative office. If possible, the department will notify students of the absence in a timely manner.

General Policy for G.I. Bill Beneficiary

Following the guidance issued by the SAA (State Approving Agency) on August 1, 2019, VIST confirms that:

- a. We allow GI Bill® beneficiaries to attend or participate in the course of education if the individual provides a certificate of eligibility under chapter 31 or 33.

- b. We permit the student to attend the course, beginning on the date the student provides a COE until the earlier date VA provides payment to the school or 90 days after the school certifies tuition and fees.
- c. We ensure that VIST does not impose any penalty, including assessing late fees, denial of access to classes, libraries, or school facilities, or require the student to borrow additional funds due to the inability to meet his or her financial obligations to the institution as a result of delayed payments for education assistance under Chapter 31 or 33, unless the student is less than 100% covered.
- d. We offer tuition relief and refunds and for reinstatement of students whose military service has required their sudden withdrawal or prolonged absence from their enrollment in the institution.

3. Tuition, Fees & Scholarships

Tuition and Fees

The following tuition and fees are in effect for the 2023-2024 academic year. School tuition and fees are set annually by the Board and are effective only for the academic year noted. The estimates of the Cost of Tuition and Fees for Attendance at the VIST are shown below.

Tuition*		
Program	Master's Degree	Certificate Program
Total Program Credits	54 Qtr. Credits	22.5 Qtr. Credits
Per Credit Hour	\$430	\$430
Per Course	\$1,935	\$1,935
Total Program Tuition	\$23,220	\$9,675

* The cost of books and supplies for the graduate program is around \$1,000. The cost of training for two certification exams (Security+ and Ethical Hacking) is also included in this tuition.

Other Fees

Application Fee:	\$75.00
Late Course Registration Fee (after add/drop period)*	\$60.00
Transfer Course Evaluation Fee (Per Transcript)*	\$100.00
Replacement Diploma	\$100.00 [#]
Student ID Card Reprint*	\$10.00
Transcripts per Copy*	\$25.00
Returned Check Fee*	\$35.00
Graduation Fee (Regalia, Diploma, etc.)	\$125.00
International Student Transfer Out/Withdrawal Fee*	\$250.00
Foreign Transcript Evaluation Fee*	\$140.00
I-20 Mailing Fee (required for I-20 forms mailed outside of the U.S.)*	\$100.0
Late Payment Fee*	\$50.00
Tuition Payment Plan Fee*	\$50.00

*Non-refundable fees

[#]Not applicable to students registered under Veterans Benefits, Chapter 36, Title 38, U.S. Code.

Cancellation & Tuition Refund Policy

The School follows the guidelines set forth by SCHEV as described under 8VAC40-31-160 N (1-12).

Cancellation of Enrollment Agreement: All monies paid by the applicant, including the application fee, if requested within three business days after signing an enrollment agreement and making an initial payment will be refunded. A student may cancel the Enrollment Agreement without any financial penalty prior to the end of the add/drop period. Later cancellations should follow the school's refund policy. Any tuition payment will be refunded to the student within a 45-day period following his/her cancellation notice. Applicants who have not visited the school prior to enrolment will have the opportunity to cancel enrollment without penalty (receive a refund of all money paid) within three business days following either the regularly scheduled orientation procedures or following a tour of the school facilities and inspection of equipment where training and services are provided.

Please note that the school will only issue tuition refunds to the organization or person who made the original payment. The application fee and the postage fee are not refundable. In order to get a full refund a written or verbal notice must be

received by the last day of add/drop period. In case of no notice, the last day of attendance will be determined within 14 calendar days after the student stopped attending. See “unofficial withdrawal” below.

VIST will issue refunds to students who have terminated their status as students within 45 days after receipt of a written request or the date the student last attended classes, whichever is sooner. Following refund schedule is used to determine any refunds VIST owes to the students in case of dropping a course or withdrawing from the school.

Time of withdrawal Written notice	Tuition refund amount*
Up to the last day of add/drop period	100% of the quarter tuition
After the add/drop & through 25% of the quarter	50% of the tuition
After 25% and through 50% of the quarter	25% of the quarter tuition
After 50% of the quarter	No refund will be issued

* Excludes all fees

VIST will refund any money, including advance deposit paid on behalf of any students, including veterans, according to the refund schedule in the table above.

An official withdrawal is when a student submits an application to withdraw to the Office of the Registrar or when the student withdraws from all of his/her classes. In this case, the date of last attendance will be the day student submitted the withdrawal notice to the school, as the day of determination.

An unofficial withdrawal is when a student stops attending all his/her classes during the quarter, does not follow the college procedure to officially withdraw as outlined by the Office of the Registrar, and fails to successfully complete the term (i.e., receives all final grades of F, W, WA, U, AW, NG, FN or a combination of both). The last day of attendance will be determined within 14 calendar days after the student stopped attending.

For Veteran Students Only:

In order to comply with CFR §21.4255(a)(5), VIST has designed a refund policy based on pro-rata in nature for veterans and other eligible persons. This means that the amount of the refund will be based on the total completed portion of the program in 10% increments.

Military veterans and members of their families are subjected to the following special refund policy:

Proportion of Total Program Taught by Official Withdrawal Date	Tuition refund
Withdrawal up to the last day of add/drop period	100% of the quarter tuition
Withdrawal after 10% of hours completed	90% of the tuition
Withdrawal after 20% of hours completed	80%
Withdrawal after 30% of hours completed	70%
Withdrawal after 40% of hours completed	60%
Withdrawal after 50% of hours completed	50%
Withdrawal after 60% of hours completed	40%
Withdrawal after 70% of hours completed	30%
Withdrawal after 80% of hours completed	20%
Withdrawal after 90% of hours completed	10%
Withdrawal after 91% of hours completed	No Refund

Additionally, the VA requires, per CFR 21.4255(a)(6), that the refund be provided in no more than 40 days.

In the event that a military member must leave and withdraw from the school to due military service during an academic term:

Pending Grades: In order to protect the student's academic welfare, no grades will be issued for any class. The academic transcript will show “W” indicating that the student withdrew from the class. For Veterans, the “W” grade will not have any impact on their SAP progress report. No punitive grade will be issued.

Tuition/Deposit Refund: In the event of mandatory military deployment, VIST will refund 100% of all deposit and payment, if any, back to the student. All other withdrawals or cancellations are subjected to the pro-rata refund schedule specifically designed for the Veterans, as shown above.

Deferral of Enrollment: A member of the military in this situation can defer enrollment cumulative up to five years from the date of withdrawal or up to three years after finishing the military service.

Reinstatement to the school and program: When a student returns from his/her military services, the student will be reinstated to the same program and will be allowed to register for courses as early as the next academic term. When these students provide notice of intent to return:

- a. They will be allowed to return to the same program if the cumulative absence is no more than five years, and
- b. They will be allowed to enroll if they intend to return to the program no later than three years after the completion of the period of military service.
- c. These students will be subjected to the old tuition and refund schedule published during the year when they first enrolled at the school, prior to their withdrawal.

VIST will provide free advising services for the students to:

- a) to determine the impact of absence from the program on the ability to resume study, and
- b) to advise the student of his or her options when a program is no longer available or suitable

Late Payment Fee

A grace period of 5 working days is allowed after to the beginning date of the term. Afterward, there will be a penalty for late payment of tuition and fees. The late fee will be \$50.00. Cash, money orders, credit cards, and checks are accepted for payment of tuition and applicable fees. Late fees are not applicable to students registered under Veterans Benefits, Chapter 36, Title 38, U.S. Code. The late fee can be charged when a student missed a payment date in his/her installment or payment plan.

The payment of tuition and fees by veterans are governed by Veteran Benefits, Chapter 36, Title 38, U.S. Code.

VIST Scholarship

The Board of Directors at VIST awards two types of scholarships for academically outstanding students. The scholarships are applied towards tuition only and prorated over 4 academic terms. The following scholarships are available in 2023-24 academic year:

Presidential Scholarship: Students are eligible if they receive a bachelor's degree in computer science or related IT major from an accredited university or college with a GPA of 3.9 or above (on a 4.0 GPA scale) and enroll at VIST as full-time students with 9 credit hours per quarter. Students also must keep their GPA of 3.9 or above in order to continue to receive this fellowship award. Students who receive a Presidential Scholarship award will be granted \$5,000 per year. VIST will fund 1 Presidential Scholarship each term, totaling 4 annually.

Dean Scholarship: Students are eligible if they receive a bachelor's degree in computer science or related IT major from an accredited university or college with a GPA of 3.75 or above (on a 4.0 GPA scale) and enroll at VIST as full-time students with 9 credit hours per quarter. Students also must keep their GPA of 3.75 or above in order to continue to receive this scholarship award. Students who receive a Dean Scholarship award will be granted \$2,000 per year. VIST will fund 1 Dean Scholarship scholarships each term, totaling 4 annually.

2022 Cybersecurity Opportunity Tuition Assistance:

To promote cybersecurity education and attract potential students with interest and academic ability in the field of cyber defense, during the Fall term of 2022, VIST will offer Cybersecurity Opportunity Tuition Assistance (TA). The TA of \$3,000 will be provided only to new students who are transferring in good academic standing from other graduate programs from accredited American universities. The TA will be applied towards the tuition cost, divided into 3 payments of \$1,000 per term during the first academic year at VIST. A student must remain enrolled full-time during the first academic year to qualify. The TA is limited to only 10 new students for the Fall term. The selection is based on the date of applications for the TA. Once the limit is met, students can no longer qualify for the TA.

4. Academic Policies

Quarter and Credit System

VIST operates on a quarter-credit system allowing students to attend courses year-round and finish degree programs quickly. The academic calendar year is divided into four, ten-week terms, with each course equaling 4.5 credit hours.

Many courses at VIST are designed to be a combination of lecture and laboratory instruction. **Students should expect to spend a minimum of two hours studying or completing assignments outside of class for every hour spent in class or under direct faculty instruction.**

One Quarter Credit Hour can be earned by successfully completing **10 contact hours** of learning during the 10-week quarter. **One contact hour** of learning is defined as a minimum of **50 minutes of supervised** or directed instruction and appropriate break(s). For example, for a 4.5 credit course, a student must receive 45 contact hours of classroom instruction. **1 Credit Hour=10 Contact Hours=20 Lab Hours=30 Externship / Practicum Hours.**

Calculation of Credit

A grade is reported for each course in which a student has enrolled to indicate the quality of performance in that course. A student's academic progress will be measured according to the following scale:

<u>Grade</u>	<u>Quality Points</u>	<u>Percent Grade/Significance</u>
A	4.00	93 - 100
A-	3.75	90 - 92
B+	3.50	87 - 89
B	3.25	83 - 86
B-	3.00	80 - 82
C+	2.75	76 - 79
C	2.50	70 - 75
F	0.0	Failure
AU	0.0	Audit
I	0.0	Incomplete
R	0.0	Repeat
S	0.0	Satisfactory
U	0.0	Unsatisfactory
W	0.0	Withdrawn

Notes regarding grades:

- Graduate level courses do not recognize a D (or lesser) grade for a student enrolled in any course carrying graduate level credit. According to the regulations of any graduate level program or higher, grades lower than C are recorded as F. Any combination of two or more C or F grades will mandate an academic review by the Academic Affairs Office. Please see Repetition of Courses below for details.
- An incomplete (I) may be given in lieu of a grade when circumstances beyond a student's control have prevented completing a significant portion of the work of a course within the allotted time. The student's performance in the course must otherwise be satisfactory. An incomplete must be removed in a manner and within the time determined by the instructor. It may not be continued beyond one quarter from the end of the quarter in which the (I) is given. Failure of the student to remove the (I) by that date will result in an automatic grade of F being placed on the student's permanent transcript. An (I) cannot become a withdrawal (W).
- Satisfactory and Unsatisfactory grades will be given only for classes using the Satisfactory/Unsatisfactory Grading Option.

Grade Point Average (GPA)

The total quarter hours in which grades of A, B, C, and F have been received at this institution divided into the corresponding total quality points earned constitute the student's cumulative grade point average (CGPA). Likewise, the student's GPA for any time period is found by dividing the credit hours in which grades other than S and U were received into the total quality points earned during that period.

The student's GPA indicates scholastic standing. Factors like effort, self-esteem, or placement prospects will be regarded as extraneous to the determination of grades.

Graduation Requirement

Master's degree programs require successful completion of a minimum of 54 quarter credit hours with a minimum 3.0 CGPA.

The normal length of time for completing a master's degree is 24 months, including annual vacation.

The normal length of time for completing a graduate level certificate program is 9 months.

Students should meet the following minimum requirements to qualify for a degree:

	Master of Science in Cybersecurity & Info Assurance	Graduate Level Certificate Programs
Minimum Passing Grade Per Course	C	C
CGPA	3.00	3.00
Total Required Credits	54	22.5

In the event a student's CGPA is less than 3.0, students cannot graduate. The student should consult with the program director to repeat one of the courses for which the earned a "C."

Satisfactory Academic Progress (SAP) Policy

The following standards and requirements of satisfactory academic progress apply to all enrolled students.

1. Maximum Time Frame (MTF) Allowed

The Maximum Time Frame (MTF) is the time allowed for a student to complete a course of study. According to U.S. Department of Education standards, "The Maximum Time Frame is not to exceed 150% of the normal program length". In practice, this means all students at VIST must complete their programs of study within 1.5 times the program length as measured in quarter credit hours attempted. If a student cannot complete the program within the MTF, the student will be dismissed from the school.

All registered hours at the end of the add/drop period will be counted in the MTF determination. In addition, all transfer credit hours accepted from other institutions will be counted in the Maximum Time Frame.

The MTF is 1.5 times the Normal Program Length (NPL) which can be formulized as $MTF = 1.5 \times NPL$. For example, MSCIA program requires successful completion of 54 quarter credits to graduate with a master's degree. $MTF = 54 \text{ credits} \times 1.5 = 81 \text{ credits}$ (maximum time allowed for a master's degree program).

Program of Study	NPL in credits	MTF Allowed in credits*
Master of Science in Cybersecurity & Information Assurance	54**	81
Graduate Level Certificate Programs	22.5	33.75

*MTF includes credits attempted at VIST and transferred to VIST from other institutions

** Beyond the program prerequisites (if any)

If a student is unable to complete the program within the aforementioned time period, the individual will not be eligible to receive the original credential (i.e., master’s degree).

2. Required Minimum Completion Percentage

VIST will evaluate the successful course completion percentages for all enrolled students at 25%, 50%, 75%, and 100% of the Maximum Time Frame above to determine whether the student is maintaining specific qualitative and quantitative minimums in order to avoid probation or dismissal.

Credits Attempted: A credit attempted is defined as any credit hour (or the equivalent) for which the student has incurred a financial obligation.

Evaluation Points (% of MTF attempted)	Required Minimum Completion % (all credits attempted)
At 25% of MTF	*55% (min grade “C” or above from all graduate courses attempted)
At 50% of MTF	**60%
At 75% of MTF	**65%
At 100% of MTF	**70%

* A student not meeting standards does not have to be dismissed; probation is required.

** Probation is not allowed at this point and academic dismissal is required.

In practice, this means that when the attempted credits are 25% of the MTF, the student must successfully complete 55% of all credits attempted with a grade of C or above. Failure to meet this requirement will result in academic probation. Academic probation is permitted at this point only. Failure to meet the minimum completion percentages at 50%, 75%, or 100% renders the student ineligible for probation, and the student must be dismissed. All courses, including withdrawals and retakes, will be included in credit hours attempted. Therefore, withdrawals and retakes will have an impact on the minimum completion percentage. The completion percentage is calculated at the end of each quarter.

3. Required Minimum CGPA

The third requirement of acceptable satisfactory academic progress is to meet the minimum CGPA requirement at each evaluation point of the MTF. VIST uses a 4.00 scale grading system, and GPAs are calculated at the end of each quarter. Withdrawals are not included in GPA calculations. However, in the case of retakes, only the highest grade is included in the GPA calculation.

Evaluation Points (% of MTF attempted*)	Required Minimum CGPA For All Graduate Level Programs	
	Probation Point	Dismissal Point
At 25% of MTF	CGPA < 2.25	No dismissal is allowed. Probation is required.
At 50% of MTF	CGPA < 2.50	CGPA < 2.25
At 75% of MTF	CGPA < 2.75	CGPA < 2.50
At 100% of MTF	No probation is allowed. Dismissal is required.	CGPA < 3.00

* If these evaluation points fall during the middle of a quarter, the evaluation will be conducted at the end of the previous quarter. The Institute will not wait until the end of the next quarter to monitor the satisfactory academic progress of its students.

In practice, this means when a graduate student’s attempted credits are 50% of the MTF, a CGPA equal to or greater than 2.50 and below will result in probation, while a CGPA below 2.25 in this situation results in dismissal.

At 100% of the MTF, or graduation, whichever occurs sooner, the student must have completed all the program requirements with a CGPA of 3.00 or higher in a master’s degree program. The student who falls below the statutory

minimum is not considered to be maintaining satisfactory progress; so, no probation is allowed at this point, and the student will be dismissed from the program. She/he cannot receive the original credential.

If a veteran student fails to make satisfactory progress (failure to obtain minimum CGPA at each MTF point), and as a result goes to probation, VIST will inform the SAA within 2 weeks or before the beginning of the next term, whichever is sooner, about the status of the student. As a standard procedure, students on probation at VIST will be reported to the SAA to limit their benefits under Gi Bill® until the student is reinstated as a full-time student.

Effects of Incomplete “I” Grade on SAP

Students may request a grade of incomplete (I) from their instructor. In order to request an incomplete grade, students must have been active in the course unless extenuating circumstances can be demonstrated. Requests must be made on or before the last day of the course. If the instructor denied the request, the student may appeal to the Program Lead. If approved, the instructor informs the student of the required work and deadline, the designated department representative, and the Office of the Registrar. A student is required to make up any incomplete course work within 2 weeks of the conclusion of the course.

A grade of “I” is not included in the calculation of the CGPA but will count as credit hours attempted for calculating the successful course completion percentage. Courses that remain as an “I” at the end of the 2nd week of the following quarter will automatically become an “F” and will be calculated in the CGPA. Incompletes are also counted in the calculation of the successful course completion percentage if the student was charged for any portion of the course. Incompletes and withdrawals may have an adverse effect on the successful course completion percentage of a student if he/she has been charged tuition for any part of the course. The “I” grade is issued for verifiable, unavoidable reasons. Since the “I” grade extends enrolment in the course, requirements for satisfactory completion will be established through student/faculty consultation and documented on the student’s transcript. The instructor may complete a **Grade Change Form** to change a grade and submit the form to the Registrar’s Office on or prior to the deadline stipulated in Academic Calendar.

If a veteran student must leave the program due to military obligation, VIST applies the following policy:

In order to protect the student's academic welfare, no grades will be issued for any class. The academic transcript will show “W,” indicating that the student withdrew from the class. For Veterans, the “W” grade will not have any impact on their SAP progress report. No punitive grade will be issued. For more detail, see the Cancellation & Refund Section of the Catalog.

Effects of Repeat Course “R” on SAP

If a student repeats a course and completes it with any grade other than the grade of “F,” the following rules will apply in posting the student’s cumulative record:

1. The original grade, credit hours, and subsequent repetitions must be calculated as credits attempted in the successful course completion percentage for satisfactory academic progress. As a general rule, all of the credit hours for which the school has collected any tuition, whether for a first time or repeated course, will be included in the computation of the successful course completion percentage.
2. The GPA will be based only upon the higher grade for the repeated course attempted.
3. The original grade for the course repeated under this rule will remain on the student’s academic record. The lower attempt will be flagged for exclusion in the GPA calculation, and the higher attempt will be flagged for inclusion in the GPA calculation.
4. Course repetition does not extend the maximum time frame for completing a program of study. (Maximum Time Frame is the time allowed for a student to complete a course of study. This requirement is discussed in more detail in other sections.) The student must complete the program within the original Maximum Time Frame allowed for their program.

Effects of Transfer Credits “TC” on SAP

When a student brings credits from other institutions, these credits will be noted with a grade of “TC,” meaning *Transfer Credits*. Since these courses will not carry grades, they will not affect GPA calculations. These courses meet graduation requirements only. The student’s new normal program length will be shortened to reflect the transfer courses, and the maximum time frame will be recalculated. Normally, a transfer student would start with a 0.0 CGPA, and 0% courses attempted and successfully completed for the purpose of satisfactory academic progress.

As a general rule, a transfer student must complete at least 51% of the credit hours required by their program of study in residence at VIST. A minimum of a 3.0 grade point average (B) out of 4.0 must have been earned on all graduate-level transferable credits.

Transferable credit is considered upon the request of the student at the time of initial registration. An official copy of all transcripts from higher education institutions must be submitted to the Admissions Office to be forwarded to the Registrar for evaluation. Additional documentation such as course descriptions, syllabi, and academic catalogue may be necessary to assure that the transferred course is equivalent to one of the courses required to complete the degree program at VIST.

Effects of Withdrawals “W” on SAP

“W” grades are not calculated in the CGPA. However, they will be considered credits attempted if the student has incurred a financial obligation for the course. “W” grades affect the successful course completion percentage. A student who does not withdraw from a course before the last day to do so will receive a letter grade based upon his/her performance in the course. To withdraw from a course, the student must complete the relevant section of the Course Add/Drop/Withdrawal Form, obtain his or her faculty signature, and submit the completed form to the Registrar’s Office.

Academic Warning

Any student who:

1. Fails to maintain a minimum GPA of 3.00 in a master’s degree program for any quarter, or
2. Who receives an “F” or incomplete “I” grade; or
3. Who engages in academic dishonesty, as defined in the Academic Catalog below, will receive an academic warning at the end of that quarter. The student will continue to receive warnings until the situation improves. The Registrar has the authority to place on academic probation any student who receives warning letters for three consecutive quarters.

If a veteran student fails to make satisfactory progress (failure to obtain minimum CGPA at each MTF point), and as a result goes to probation, VIST will inform the SAA within 2 weeks or before the beginning of the next term, whichever is sooner, about the status of the student. As a standard procedure, students on probation at VIST will be reported to the SAA to limit their benefits under Gi Bill®, until the student is reinstated as a full-time student.

Academic Probation

Students who fail to maintain the required CGPA and successful course completion percentage minimums at 25%, 50%, and 75% of the Maximum Time Frame (MTF) at the end of each academic year (for those programs equal to one year in length or longer) will be placed on academic probation as shown in the table below:

Evaluation Points (% of MTF attempted*)	CGPA Falling in Probation Period for all Graduate-Level Programs
At 25% of MTF	CGPA <2.25
At 50% of MTF	CGPA between 2.25 and 2.50
At 75% of MTF	CGPA between 2.50 and 2.75
At 100% of MTF	No probation is allowed. Dismissal is required.

Students who do not maintain satisfactory academic progress will be placed on academic probation for one quarter. The student on academic probation will be advised and given assistance, if needed, in order to improve his/her CGPA. The statement “Placed on Academic Probation” will be entered into the student’s permanent record. The academic probationary period is normally one quarter. The student is considered to be maintaining satisfactory academic progress while on probation.

Academic Dismissal

Students who do not maintain at least a 2.00 GPA in the graduate program at the end of the academic probationary period and who cannot meet the minimum CGPA requirement at the evaluation points shown in the table below, will be dismissed from the school.

Evaluation Points (% of MTF attempted*)	Dismissal Points for all Graduate Level Programs
At 25% of MTF	No dismissal is required.
At 50% of MTF	CGPA < 2.25
At 75% of MTF	CGPA < 2.50
At 100% of MTF	CGPA < 3.00

The statement “Academic Dismissal” will be entered into the student’s permanent record. Academic dismissal normally is permanent unless, with good cause, students reapply and are accepted under special consideration for readmission by the Institute. (See “Reinstatement as a Regular Student” policy below.) In addition to Academic Dismissal, the school reserves the right to dismiss a student for violating the student code of conduct.

Appropriate tuition refund, if applicable, as stated in this Catalog, will apply to all dismissed students as well as those who withdrew.

If academically dismissed, any students receiving the GI Bill® support will lose the benefit immediately. In order to regain eligibility student must be officially reinstated as a regular student according to the following policy.

Reinstatement as a Regular Student

A student who has been dismissed from the VIST may petition to be readmitted. In order to be considered for readmission, the student must submit a written petition which describes the changes in behavior or circumstance that will result in improved academic performance. The readmission petition must be forwarded to the Director of Education at least two weeks before the beginning of the quarter in which the student requests readmission. In coordination with the Registrar, the Director of Education will determine if the student has demonstrated a likelihood for future success in the program of study. If the Institute determines that there is a likelihood of future success, the student will be placed on academic probation for a period of one quarter. The student may then be permitted to retake previously failed, incomplete, or withdrawn courses to improve his or her CGPA and course completion percentage and re-establish satisfactory academic progress. During the academic probationary period, these students may not be eligible to receive loans, grants, including Title IV and or GI Bill® benefits, and as such, they will be responsible for all costs incurred during the probationary quarter.

At the completion of this academic probationary quarter, a student who has established satisfactory progress according to the tables above will return to regular student status.

If a veteran is dismissed from the school due to failure to make satisfactory academic progress, the following procedure is followed for reinstatement.

1. The veteran must submit written petition to VIST describing the changes in his/her circumstances that will result in improved academic performance
2. If the president office determines a likelihood of future success, then the student will be re- admitted as a probationary student.
3. Such student will be placed on probation during the first term. Students on probation are not allowed to enroll full course load.
4. During the probationary term, the student must repeat lower grade course(s) to improve his/her term GPA. The probationary period is only one term. Failure to obtain a satisfactory GPA will result in permanent dismissal.
5. If a student can obtain a term GPA of 3.0 at the end of the probationary period, then the student will be reinstated as a full-time student and will be allowed to enroll full-time during the following term. At this point, VIST will inform the SAA about the reinstated status of the dismissed student so that his/her benefits under the GI Bill® benefit continues.

Attendance Policy

Successful course completion in residential (face-to-face) instruction depends upon routinely following the instruction and guidelines provided in the course syllabus. The student's class attendance will be monitored by timely completion or submission of weekly course assignments/requirements such as course projects, presentations, reports, group discussions, demonstration of learning, and knowledge retention. A record of excused and unexcused absences, as well as attendance, will be maintained by the corresponding faculty member. Excused absences are for example: documented medical appointments or leaves, funeral, legal obligations, religious observations, and military obligations. When requested by the student, teachers will inform the student who has been absent whether make-up work is allowed and whether absences jeopardize the student's academic standing in a class. Students are also expected to arrive to class on time and not leave before class is dismissed.

A student that misses 45 minutes or more of scheduled class time is marked absent. Absence for unexcused reasons may negatively affect the student's final course grade. More importantly, under faculty discretion, excused and unexcused absences in excess of 25% of total class and lab time may result in failure of the course. All students are expected to arrive to class on time. Late attendance is disruptive to both the instructor and students. If a student is tardy for a class more than the instructor deems advisable, the instructor might report the issue to the student's Program Lead for appropriate action.

Grade Appeal Policy

The student must initiate a grade appeal within 1st week of receiving the grade by submitting a written request to the instructor. Any grade change request made after that time period will not be honored. If faculty and student cannot resolve the issue, the student is required to submit an official Grade Appeal Form to the Program Lead no later than the end of the 2nd week. The Program Lead will call for a grade appeal meeting whose members are the Director of Education, Registrar, and a faculty member. During the grade appeal hearing, the student and the faculty member may present information. Grade Appeal meeting decision is final and not appealable.

5. Student's Rights and Responsibilities

VIST is committed to maintain fair and reasonable practices in all matters affecting students: the delivery of educational programs, provision of support services, and timely resolution of disciplinary matters, as well as the handling of student grievances. Furthermore, VIST endorses and supports the basic principles of the Codes of Ethics issued by the American Association of Collegiate Registrars and Admissions Officers (AACRAO). Student understanding and cooperation are essential to the successful implementation of this legal structure.

Students are fully protected against impulsive, subjective, unreasonable, unauthorized, false, malicious, unfair, or inappropriate evaluations or unacceptable behavior by a faculty member. Student complaints as considered as grievances that can be classified as Academic (dealing with term Grades or Grade Point Average), Non-Academic, and Discriminative Complaints (dealing with sexual harassment, illegal discrimination, or violation of VIST Regulations or Policies, etc.).

Students, staff, and Academic Advisors are required to act in ways that promote the safety of self and others and report any serious crimes and emergencies to the administration as soon as they are known or discovered.

Freedom of Access

VIST is open to all qualified applicants according to its published admissions policies and standards. Upon enrollment, students have access to all VIST services, physical facilities, and resources. Access will be denied to individuals who are not VIST students.

Sexual Harassment Policy

As an institution of higher education, VIST will not tolerate any form of sexual harassment as VIST provides educational programs, employment, and a business environment free of unwelcome sexual advances, requests for sexual favors or intimidation, and other verbal or physical conduct or communications, including electronic communications and systems, constituting sexual harassment as defined and otherwise prohibited by State and Federal statutes. Any individual who knowingly violates this Policy will be subject to appropriate and immediate disciplinary action.

Formal Grievance Procedure

VIST has a Grievance process and procedures for students to file grievances as well as an appeal process to assure protection of student rights and maintain fairness and objectivity. Students have the right to appeal any adverse academic decision, standard, or requirement if any of the following conditions exist:

- A faculty who issued a course grade by mistake, fraud, bad faith, or retaliation.
- Extenuating circumstances make it impossible to comply with the standard or requirement
- An undue hardship would result from a strict application or interpretation of a standard or requirement.

Documentation will be required, and timely processing of the grievance will be taken into consideration. If a student appeals an academic standard or requirement, the President will handle the appeal.

The purpose of the appeal process and procedures is to provide a system that will represent “fairness and the absence of arbitrariness.” VIST makes every effort to assure that its grievance procedures are clear to students and the process is not burdensome or cumbersome.

VIST faculty and staff attempt to create, in all areas, an atmosphere that is conducive to learning. For this reason, we have established a procedure that we hope will address any school-related problem, concern, or complaint. Students may express concerns to any administrator. Complaints, however, are best handled by following the below procedure.

Step 1: Most academic concerns will be handled by the instructors. Students should first discuss the problem with the instructor.

Step 2: If the problem is not resolved at that level, the student should contact the Lead Faculty member of the program or the Director of Education. All administrative staff members maintain an open-door policy.

At the student's written request, an ad hoc Grievance Committee (GC) comprised of the President, Director of Admissions, Lead Faculty members, and Title IX Coordinator (if applicable) will be convened to address concerns that remain unresolved. The ad hoc Grievance Committee will convene within 10 days of a written request. The student will be notified of the committee's decision within three days of the meeting.

If there is a finding of inappropriate behavior, prompt disciplinary action, including possible termination or expulsion, will be taken.

- Withdrawal of a complaint will not necessarily result in the termination of the school's investigation into the allegations.
- False and malicious charges may result in sanctions being imposed against the complainant by the school and may lead to charges being filed against the complainant by the accused.

After a judgment has been rendered, either party may choose to avail himself/herself of the established grievance procedures:

When any investigation of a complaint of sexual harassment is completed, the file containing all documentation relating to the complaint will be maintained in the Human Resources Department in a separate confidential file.

Documentation on any disciplinary action will be maintained in accordance with the following guidelines:

- (a) Documentation will be maintained in the Student's file, which resides Registrar Office
- (b) Documentation will be maintained in the Professional and Support Staff's personnel file, maintained in the Human Resources Department.
- (c) Documentation will be maintained in the Faculty's personnel file in the Human Resources Department.

After following the above stated procedure, if the student feels that his or her concerns have not been resolved, he or she may address these concerns in writing to the regulatory agencies listed below:

Schools accredited by the Accrediting Commission of Career Schools and Colleges must have a procedure and operational plan for handling student complaints. If a student does not feel that the school has adequately addressed a complaint or concern, the student may consider contacting the Accrediting Commission. All complaints reviewed by the Commission must be in written form and should grant permission for the Commission to forward a copy of the complaint to the school for a response. This can be accomplished by filing the ACCSC Complaint Form. The complainant(s) will be kept informed as to the status of the complaint as well as the final resolution by the Commission. Please direct all inquiries to:

Accrediting Commission of Career Schools & Colleges
2101 Wilson Boulevard, Suite 302, Arlington, VA 22201
(703) 247-4212, www.accsc.org

A copy of the ACCSC Complaint Form is available at the school and may be obtained by contacting (name/position) or online at www.accsc.org.

Any issues or problems which have not been satisfactorily answered or resolved by VIST may also be directed to the:

State Council of Higher Education for Virginia (SCHEV)
101 N. 14TH St., James Monroe Bldg. - Richmond, VA 23219
Tel: (804) 225-2600 and Fax: (804) 225-2604; www.schev.edu

The student will not be subject to unfair treatment or adverse actions by the school as a result of initiating a complaint proceeding.

Notice for GI Bill® Beneficiaries:

The Virginia State Approving Agency (SAA) is the approving authority of education and training programs for Virginia. Our office investigates complaints of GI Bill® beneficiaries. While most complaints should initially follow the school grievance policy, if the situation cannot be resolved at the school, the beneficiary should contact our office via email at saa@dvs.virginia.gov. *GI Bill® is a registered trademark of the U.S Department of Veterans affairs (VA). More information about education benefits offered by VA is available at the official U.S government website at <http://www.benefits.va.gov/gibill>.*

Civil Rights Compliance

In compliance with Federal, State, and local government requirements and the Civil Rights Act of 1964 as amended, VIST will not discriminate against any individual on the basis of age, sex, race, color, religion, association, national and ethnic origin, marital status, sexual orientation, medical condition or physical disability, or qualified disabled veterans in the administration of its educational programs, institute-administered programs, publications, admissions of students, award of scholarship and loan programs or in its employment practices.

Catalog of Record

VIST reserves the right to change its educational programs, academic requirements, course offerings, schedules, policies, rules, regulations, tuition, and fees, in compliance with the SCHEV regulations, or to make other changes that the Institute considers essential and necessary to its continued successful growth.

Although every effort has been made to ensure the accuracy of information provided in this Catalog, students who use this publication are encouraged to notify VIST of any printing errors or information inaccuracy. This request is in support of VIST's deep commitment to providing comprehensive information to students.

Privacy of Student Records

VIST is not participating in the Family Educational Rights and Privacy Act (FERPA), also known as the "Buckley Amendment." This program is for colleges and universities who receive federal funding. Currently, VIST is not a Title IV school and does not receive any federal funding. Nevertheless, VIST strives to do the best to protect the privacy of student records.

Retention of Student Records

A detailed system of records is maintained for each enrolled student. A student's file will minimally contain application documents, admissions credentials, enrollment, and attendance records, course grades, satisfactory academic progress records, written communication with the student, any disciplinary actions taken, and other pertinent documents. VIST shall retain student academic records permanently in accordance with the guidelines published by the State Council for Higher Education of Virginia (SCHEV). Fireproof storage shall be used for the safekeeping of students' records, including records of graduation and degree(s) granted. If stored on computers, such records will have backups and remain the permanent property of VIST. They shall not be available for loan or release to third parties without the written consent of the appropriate student.

Non-Discrimination Policy

VIST provides its constituents' opportunities for the pursuit of excellence through its educational programs and services. VIST offers open access to its programs and support services without regard to race, color, age, gender, creed, national or ethnic origin, marital status, sexual preference, physical disability, or any other legally protected status in the administration of its educational programs, admission of qualified students or offering of any Institute-administered activities.

Copyright Law

Faculty, staff, and Students are required to comply with federal copyright law. The United States Copyright Law protects all copyrighted materials: Printed materials (including copyrighted electronic versions), such as books and journals, music, sound recordings, films, videocassettes, art works, and computer software. Most Internet sites and all their contents are protected by copyright, unless otherwise noted. The Copyright Act of 1976 grants copyright owners exclusive rights to publish, reproduce, perform, and display their works. Anyone publishing, reproducing, performing, or displaying all or part of a copyrighted work is guilty of infringing the copyright unless the act falls within one of the fair use exceptions, or unless she or he has acquired permission to use the work from the copyright owner. In other words, students must not copy other materials or concepts, and if referring to existing materials, they should properly cite those materials. More information about the copyright law may be available at <http://lcweb.loc.gov/copyright>.

Student's Code of Conduct

Students are expected to maintain themselves at all times in a manner befitting a professional institution. VIST encourages professionalism in all its constituents. Each student is expected to be an example of proper conduct. This includes the student's attitude and actions during all phases of the student's academic life. The administration of VIST has the authority to take appropriate action or administrative disciplinary measures for the violation of this Code of Conduct.

All members of VIST have a responsibility to protect academic excellence and ensure that scholarly probity and standards of conduct are maintained. Furthermore, faculty and staff are responsible for coordinating and supervising students' academic work to encourage honest and individual effort and take appropriate action if instances of academic dishonesty are reported or discovered.

Upholding academic honesty is primarily the responsibility of each learner. VIST views any violation of academic integrity (cheating, plagiarism, falsification, etc.) as a voluntary act for which there is no acceptable excuse.

1. Academic Misconduct

Violations to the Code of Conduct can ultimately lead to the improper evaluation of assessment tasks leading to unjust attribution of grades or course status. Therefore, it is integral to monitor and evaluate any allegation of academic misconduct. Forms of violation can include, but are not limited to the following:

1. Unauthorized use of material or improper collaboration
2. Intended or unintended plagiarism
3. Submissions of the same work for multiple courses
4. Falsifying, purchasing, or altering the work of others or representing others' materials as one's own work
5. Unauthorized access to or the theft of the work of others

2. Non-Academic Misconduct

VIST students should remember that the following types of behaviors are prohibited and that being found guilty of engaging in them can serve as grounds for certain sanctions, including expulsion or the involvement of the local police department.

1. Copyright infringement: Most printed materials, photographs, motion pictures, sound recordings, and computer software are protected by copyright. Copyrighted works may not be reproduced, distributed, performed, or adapted by students without the copyright owner's permission.
2. Computer / Internet misuse: Some software products are protected by copyright laws. Students may not copy the institution's software without the permission of the copyright holder
3. Physical and psychological abuse: Any form of physical and/or psychological abuse, threat, or harassment of another person or fighting on school property will result in sanctions. If the abuse is judged severe enough, the local police department may be consulted.
4. Property damage: Littering, defacing, destroying, stealing, or damaging school property (or attempting to do so), initiation thereof, or causing such damage to be initiated is prohibited. Any false report, warning, or threat of fire, explosion, or other emergency under the school's jurisdiction is also prohibited.
5. Gambling: Gambling or holding a raffle or lottery at the school without proper approval is forbidden.
6. Obscene language or conduct: Use of profanity and disorderly or obscene conduct is strictly prohibited.
7. Alcohol consumption: The use, possession, or sale of any alcoholic beverage, regardless of its potency or lack thereof, is prohibited on all school property.

Furthermore, the following activities may result in an immediate school expulsion:

1. Illegal activities: Violation of any federal, state, and local laws.
2. Drug use: The manufacture, sale, dispensation, possession, or use of any controlled substances or illegal drug paraphernalia on school premises or at school-sponsored events is considered an illegal activity and is prohibited on all school property.
3. Firearms possession: The use, possession, or sale of firearms or other weapons or any dangerous explosives or explosive elements or component parts on school property is strictly prohibited.

The school does not excuse any violation of its policies on the basis that the student was not aware of these policies and their subsequent penalties and sanctions.

Students are required to comply with VIST's current Policies, Regulations, and Procedures. Any violation of Policies and Regulations established by VIST shall be addressed accordingly, which may result in disciplinary action, suspension, or dismissal following appropriate hearing and appeal procedures. Any suspended or dismissed student shall be given the right to appeal the administrative decision.

Statement of Academic Freedom

VIST is fully committed to the protection of academic freedoms to inquiry and expression in scholarly activity. A diversity of opinion, course content, and instructional and learning methods are encouraged and considered as contributing to the growth of VIST and the professionalism of its faculty. Confident in the qualifications, experience, and expertise of its faculty, VIST encourages its faculty and teaching staff to exercise their individual judgments regarding the content of assigned courses, organization of current topics, and innovative pedagogic strategies/methods, providing only that these judgments are made within the context of appropriate published course descriptions, and that the instructional methods are those officially sanctioned by the Institute.

The Institute and faculty enter into a contract in which each faculty member is entitled to full academic freedom in research, statements, and conclusions during each instruction period.

VIST makes its educational programs open to all qualified applicants according to its published admissions policies and standards. Upon matriculation, students will have access to all services and its physical facilities with a student ID number. Access will be denied to individuals who are not VIST students.

Transferability of VIST Credits

Transfer of the credits earned at VIST to another institution is subject to the terms and conditions of the accepting institution and the types of courses being considered for transfer. Acceptance of transfer credit hours from one institution to another is a prerogative of the accepting institution.

Credit for Prior Learning

The purpose of this policy is to recognize significant technical training and competency attainment that students have mastered through their professional life before they have been admitted to a degree program at VIST and to award appropriate credits for the competencies attained. However, per SCHEV guidelines, prior learning credit is not available for graduate programs.

Academic Honesty Statement of Policy

All students must be honest and forthright in their academic studies. To falsify the results of one's research, steal the words or ideas of another, cheat on an assignment, or allow or assist another to commit these acts corrupts the educational process. Students are expected to do their own work and neither give nor receive unauthorized assistance.

Academic misconduct is any other act that disrupts the educational process or provides a student with an academic advantage over another student. Academic misconduct includes, but is not limited to:

The unauthorized possession, copying, distribution, sale, or other transfer of all or any part of an academic exercise, or the answers or solutions to an academic exercise, whether or not the exercise has been administered.

Changing, altering, attempting to change or alter, or assisting another in changing or altering any grade or other academic record, including grades or records contained in a grade book or computer file, that is received for or in any way attributed to academic work;

Posting of notes or other materials from a class (whether the student is enrolled in the class or not) on the Internet, whether or not for a fee, if the faculty member has expressly prohibited the posting of such materials.

Drugs and Alcohol Policy

VIST prohibits the illegal possession, use, consumption, manufacture, sale, or distribution of drugs, alcohol, and drug paraphernalia. Any violations of this drug policy may be subject to sanctions by the VIST Conduct System and may be reported to all appropriate law enforcement authorities. The claim that the use of marijuana was for medicinal purposes will not automatically be sufficient for dismissal of any pending charges nor for a determination that the student is not responsible for violating this policy. The school facilities are designated as smoke-free for all substances.

6. Descriptions of Academic Programs

MS in Cybersecurity & Information Assurance (MSCIA)

The purpose of our MSCIA program is to meet the growing need for job-ready men and women primarily in the computer and information technology industry, with particular emphasis on the security sector.

MSCIA is designed by cybersecurity academicians and industry professionals to prepare graduates with job-ready skills. The program includes a choice of two specialization tracks: System Cybersecurity and Operation Assurance.

MSCIA Program Objectives (PO)

This program is designed to fill a domestic and worldwide critical and growing need for cybersecurity professionals in the public and private sectors. Cybersecurity is becoming one of the major domestic and global challenges. VIST focuses on providing its students with all the knowledge, abilities, and skills to “exceed emerging global challenges.” Our Master of Science in Cybersecurity & Information Assurance (MSCIA) program emphasizes the identification and mitigation of information security risks and threats faced by organizations as well as strategies for securing data, processes, and systems of these public and private institutions.

The program has been carefully designed to meet the real-world requirements and to facilitate hands-on experience for achieving successful careers in the general domain of information and cybersecurity technology. The program is appropriate for IT professionals who are interested in mid-level cyber security positions, managing the cybersecurity program, including supervising information security implications that specifically include strategic, personnel, infrastructure, policy enforcement, emergency planning, and security awareness.

General job titles available for graduates: Cybersecurity Analyst, Information Assurance Analyst, Cybersecurity Specialist, Cybersecurity Consultant, Cybersecurity Manager/Administrator, Information Security Manager, Network Security Specialist, Network Security Administrator, System Security Auditor and IT security specialist.

Program Objectives

Upon successful completion of all program requirements, graduates will be able to:

- Identify components of a modern information system and the threats that challenge its security and foundational infrastructure.
- Apply knowledge in the field of cybersecurity to propose solutions to real world problems.
- Identify and apply cybersecurity’s tools and procedures, standard-based concepts and capabilities.
- Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management, for wired and wireless networks that affect security of the cyberspace
- Develop, implement and maintain digital security strategies to protect the organization’s data.
- Evaluate and recommend cybersecurity systems, applications and solutions for a network’s defense and monitoring scheme
- Relate to and communicate technical information verbally, in writing, and in presentations.
- Use appropriate resources to stay abreast of the latest industry tools, applications, and techniques in the domain of cybersecurity

CIP Code: 11.1003

SOC Table via www.onetonline.org/crosswalk.

- 15-1212: Information Security Analysts
- 15-1211: Computer Systems Analysts
- 11-3021: Computer and Information Systems Managers
- 15-1231: Computer Network Support Specialists

Students in the Master of Science degree in Cybersecurity & Information Assurance must complete 54 quarter credit hours, as follows:

Category	# of Courses Required	Total Credits Required
Core Courses	5	22.5 Quarter Credits
Specialization	4	18 Quarter Credits
Electives	2	9 Quarter Credits
Capstone	1	4.5 Quarter Credits
Total	12 courses	54 Quarter Credits

Core Courses

Each graduate student is required to take five (5) out of nine (9) core courses, equaling a total of 27 credits. The choice of core courses does not need to be approved by an academic advisor. The following core courses do not have prerequisites. Each course is 4.5 quarter credit hours.

- CSIS 500 – Principles of Security
- CSIS 512 – Cybersecurity Infrastructures
- CSIS 518 – Cryptography & Network Security
- CSIS 520 – Strategies and Practices for Cyberspace Threats and Defense
- CSIS 528 – Network Principles and Cybersecurity Strategy
- CSIS 530 – System Assessment & Risk Analysis
- CSIS 536 – Computing Operation Systems & Cybersecurity
- CSIS 592 – Forensic Evaluation and Incident Response Management
- CSIS 594 – Legal and Ethical Aspects of Cybersecurity

Specialization Areas

Specialization areas are the fields that students may have more interest in one field than others. Specialization areas are not mandatory requirements. It is optional that students may focus on their future career development.

Cybersecurity Systems: (Choose 4 out of 5 courses. Each course is 4.5 credit hours)

- CSIS 510 – Trusted Computing
- CSIS 530 – System Assessment & Security Risk Analysis
- CSIS 570 – Enterprise Security Technologies
- CSIS 580 – Cybersecurity Intelligence/Counter Intelligence
- CSIS 650 – System Architect and Cybersecurity

Operation Assurance (Choose 4 out of 5 courses. Each course is 4.5 credit hours)

- CSIS 536 – Computing Operation Systems & Cybersecurity
- CSIS 585 – Malware Analysis and Defense
- CSIS 592 – Forensic Evaluation and Incident Response Management
- CSIS 595 – Information System Auditing and Monitoring
- CSIS 665 – Disaster Recovery & High Availability

Electives

In addition to the above core and specialization courses, students can take one or more of the following courses as their electives. (Choose 2 out of 9 courses. Each course is 4.5 credit hours)

- CSIS 540 – Introduction to Ethical Hacker Skills

CSIS 545 – Advanced Ethical Hacker Skills
CSIS 560 – Introduction to Mobile Computing
CSIS 590 – Introduction to Cloud Computing
CSIS 591 – Introduction to Digital Forensics
CSIS 593 – Advanced Applied Digital Forensics
CSIS 620 – CISSP Principles and Practices I
CSIS 626 – CISSP Principles and Practices II
CSIS 636 – Database System Management & Assurance

Capstone

Students must complete a knowledge-integrating experiential/capstone project in the last term after concluding all core and concentration courses.

CSIS 690 - Cybersecurity Capstone Project

7. Student Services

VIST believes student-centered approach that puts students' academic and social welfare at the center of daily operation.

Academic Advising

As a graduate institution, all of our students will be assigned a faculty advisor responsible for assisting in course planning and guiding the student.

Students receive academic advising at a minimum, once a quarter, as well as during the registration process. Academic advisors assist students in selecting courses appropriate for their program and schedules. At any time during the quarter, students may schedule an appointment with their academic advisor, designated department representative, or instructor for assistance. Also, students are urged to immediately contact them to discuss personal issues that may affect their academic performance. Academic advisors are also available for consultation on Satisfactory Academic Progress (SAP), preparation of professional resumes, or career advising and planning. The scope of academic advising may include:

1. Analyzing personal interests related to academic and career planning.
2. Determining the appropriate and suitable educational program for successfully achieving a chosen career or goal.
3. Selecting courses and student activities that maximize scholarly activity and potential academic success.
4. Developing a suitable academic plan that encompasses both the course workload and the supplemental needs of the students.
5. Academic progression in the pursuit and completion of required Scholarly Research activity and the Capstone Project (if applicable).

Online students may contact their academic advisors via e-mail or phone. The Institute provides academic counseling and support to students who are not meeting Satisfactory Academic Progress (SAP). Students are strongly encouraged to schedule an appointment with their Academic Advisor at least once a month and biweekly when they are on a SAP monitoring period. General contact for all academic matters is academic@VIST.us

Career Services Center

Career assistance is provided to students in pursuit of professional employment and career advancement. The Career Services Center assists students with obtaining the skills necessary for successful interviewing and provides a network of employers in each discipline. The Career Services Center offers a full range of programs to enrolled students and alumni to further their professional development and transition into career fields. To assist upcoming graduates with their job search preparation, the Institute offers the following resources:

- Resume review
- Job leads
- Job search methods
- Interview preparation and role-playing
- Career strategy development
- Career fairs
- Exit interviews

The Institute does not guarantee employment. Poor attendance, poor grades, and the inability to provide the Career Services Center with the necessary requirements can impact a student's ability to obtain employment. Students must sign an authorization form available in the Career Services Center and have a current resume on file in order to receive job assistance. In addition, graduates should notify the Career Services Center as soon as they become employed in their career field. Job search assistance is always available to alumni who remain in their field of study.

Career Services organizes a number of career events throughout the year. These include job fairs, seminars, on-campus interviews, and networking sessions. Jobs are posted on announcement boards and on the VIST website. Companies and organizations interested in participating in VIST career events are welcome to contact us. Students can get more information by visiting the Career Services page or contact us via email: careerservices@VIST.us

Social Adjustment and Coping Skills

At VIST, we care not only about academic welfare but also the social welfare of our students. We invite our students to speak with admission advisors or with lead faculty of their program to share openly and confidentially about their challenges. In order to help students with their academic challenges, we administer an “At-risk” student survey via our faculty in the middle of the quarter. This survey helps us to identify at-risk students and implement a timely intervention plan. Those students who experience emotional and social issues are invited to talk to academic advisors.

At VIST, we do not have a qualified counselor on-site, therefore, students experiencing social issues and requiring counseling are referred to external counselors. Although, VIST makes every attempt to comfort students when requested by a student about such coping skills as life skills, personal financing skills, etc. VIST refers these students to an external counselor.

New Student Orientation

VIST holds New Student Orientation (NSO) each quarter to help new students get familiarized with the processes and procedures of the Institute. It is critical that new students make every attempt to attend. Orientation gives students an opportunity to meet with their designated department representative, the Office of the Registrar, the Office of Student Accounts, and to receive Populi instruction. This is an opportunity to discuss payment, course selection and address any last-minute issues. Orientation is typically held the week before the start of the term. The Institute attempts to provide an orientation time accommodating most student schedules. Online students receive an online orientation. Upon completion of each session, students are sufficiently and satisfactorily oriented to the Institute, its equipment, services, staff, and faculty.

Student Resources

Tutoring Program: VIST offers tutoring services and academic support to all students. There is no charge to students for tutoring services. Professional and peer tutors provide tutoring on a one-on-one or group study basis.

Students requesting tutoring must attend all classes, clarify their needs with the tutor, bring all materials to tutoring sessions, share academic progress and concerns with a tutor, and complete an evaluation after completing tutoring session(s).

On-campus Activities: Student activities are scheduled throughout the year. This includes on-campus entertainment; campus sponsored mixer cookouts, cookie and pizza nights; and access to recreational, cultural, and social events. The Institute posts all activities by calendar and by social media. In addition, students are notified by e-mail and flyers.

Parking: Parking is readily available at all campuses and is free to inquiring and current students. Parking lots are lighted, well secured, and have clearly marked spaces for handicapped parking. VIST is not liable for any vehicle damage occurring in the parking lots. Students and Institute guests are responsible for their possessions at all times while on-campus.

Library and Learning Resources System (LRS)

The library contains an up-to-date collection of books, periodicals, newspapers, and other instructional materials that are readily accessible to all VIST faculty and students. The library also boasts touchscreen computers that allow faculty and students to access VIST’s Online Library. The Online Library is accessible for each student and faculty member via their Populi account. The online Library contains thousands of periodicals and books in electronic format. In addition, students have access to the librarians to assist with information search needs. Access to the Librarian is also provided via Populi.

Online librarians are available daily (except holidays) based on the following schedule:

Monday - Friday 8AM to 10PM

Saturday - Sunday 12PM to 7PM

Curricular Practical Training (CPT)

If you are an F-1 student, you have the option of training in the United States by engaging in practical training during your program or after it ends. Practical training can provide valuable work experience by sharpening and adding to the skills

you are learning at the school. There are two types of practical training available for F-1 students: Curricular Practical Training (CPT) and Optional Practical Training (OPT).

The Code of Federal Regulations 8 CFR 214.2(f)(10)-(12) states that CPT must be an “integral part of an established curriculum. The regulations define curricular practical training as an “alternate work/study, externship, cooperative education, or any other type of required externship or practicum, which is offered by sponsoring employers through cooperative agreements made with the school.”

Virginia Institute of Science and Technology offers its international students the opportunity to engage in Curricular Practical Training (CPT). CPT is work authorization for students holding F-1 visas (temporary authorization for practical training directly related to the major field of study—paid or unpaid). CPT permits eligible students to gain specialized, curriculum-based training linked to the student’s field of study. Eligibility requirements include completing one academic year of study in the United States. CPT will only be authorized for students who have a valid, verifiable training offer related to their enrolled program. Students interested in CPT can find detailed information on CPT policies, procedures, and requirements by contacting the International Students Office (ISO).

Eligibility Requirements

In order to apply for CPT (except for transfer-in students), a continuing student must maintain Satisfactory Academic Progress (SAP) as defined in Academic Catalog.

Qualified students may participate in CPT while taking their full-time academic course load. However, credit received through CPT is not applied towards a students’ graduation requirement.

A Full-Time F-1 Students	For Transfer F-1 Students	For Initial F-1 Students
Duration of Study Requirement	Must have completed: One Academic year of study in the USA	Must have completed: One Academic year at VIST (3 terms)
GPA Requirement	No CGPA requirement at the time of application. Must maintain SAP afterward.	Met minimum CGPA of the program at the time of application. Must maintain SAP afterward.
Part-Time CPT	Permitted unlimited times throughout the program	Permitted unlimited times throughout the program
Full-Time CPT	Available during vacation	Available during vacation

All students are eligible for CPT after completing one full academic year of study in the USA. If a transfer student has already completed one full academic year in their previous school, they are eligible for a CPT as early as day one at VIST. VIST imposes no limits on part-time CPT, and students are eligible for a full-time CPT during their standard vacation. There is no limitation on the length of time a student may participate in CPT, but if the student has participated in aggregate twelve months or more of full-time employment, USCIS may deny the Optional Practical Training (OPT) application or not grant a full (12 months) OPT.

CPT Fee

To apply for CPT, a student must pay a \$430 fee. The fee is charged each term a student wants to participate in a CPT. The fee should be submitted together with all documentation required for CPT. More detailed information about the CPT application process and required documentation can be obtained by contacting the DSO.

Mental Health and Suicide Prevention Lifeline

Local community offers resources and support for persons struggling with depression and suicidal thoughts. For help students can call PRS Crisis Center at 703.527.4077 or 988 available 24/7. A person can also text 85511 with a message CONNECT. PRS is a nonprofit organization providing behavioral health, crisis intervention and suicide prevention services in Fairfax County.

Fairfax County also offers Emergency and Crisis Services for people who have mental illness, substance use disorder, and/or developmental disability, are in acute distress, and need immediate help. Walk-in psychiatric services are available at the CSB (Community Services Board) Merrifield Center (8221 Willow Oaks Corporate Drive, Fairfax) 703.573.5679. There might be a fee for the services, but it is adjusted based on the individual's ability to pay. No one is refused services if they can't pay. More services and information can be found on Fairfax County website [fairfaxcounty.gov/community-services-board/](https://www.fairfaxcounty.gov/community-services-board/)

8. Course Descriptions

Academic Courses

CSIS 500 – Principles of Security in Computing (4.5 Q.crdts)

This course is the core course of the cybersecurity program. It will provide an overview of the introductory topics in cybersecurity, which will be the basis for the other security-related courses in the CSIS. Topics include basic concepts on **CIA (confidentiality, integrity, and availability)**, risk management, disaster recovery, access control, database security, and basic cryptography and software application vulnerabilities.

This course will also study the security models for cyber space (Bell-LaPadula, Clark-Wilson, Biba, and Gligor models). It analyzes and compares, with respect to formal and pragmatic criteria, the properties of various models for hardware, software, and database security. Formal specification and verification of security properties, operating system security, telecommunication security, trust management, multi-level security, security labeling, security auditing, and intrusion detection, security policy, safeguards and countermeasures, risk mitigation, covert channels, identification and authentication, password schemes, access control lists, and data fusion techniques, configuration and troubleshooting, etc. will be covered in this course.

Course Objectives:

- Understand the core cyber security/information assurance (IA) principles
- Describe the concepts of **CIA (confidentiality, integrity, and availability)**
- Describe basic risk management processes and practices
- Identify security tools and hardening techniques
- Understand OS, database, and application security threats and vulnerabilities
- Safety measure methods and technology of telecommunication
- Describe different classes of attacks
- Define types of incidents, including categories, responses, and timelines for response
- Analyze threats and risks within the context of the cybersecurity architecture
- Ensure allocate enough system memory and disk space, as well as traffic load status
- Access additional external resources to supplement the knowledge of cybersecurity
- Configuration & Troubleshooting
- The course includes a project.
- This course is 4.5 credits.
- Prerequisites: None.

CSIS 510 - Trusted Computing (4.5 Q.crdts)

This course provides an overview of the fundamental technologies behind Trusted Computing. Students will learn what Trusted Platform Modules (TPMs) are and what capabilities they can provide both at an in-depth technical level and in an enterprise context. Students will also learn about how other technologies such as the Dynamic Root of Trust for Measurement (DRTM) and virtualization can both take advantage of TPMs and be used to enhance the TPM's capabilities.

This course will cover major use cases for trusted computing, including machine authentication, data protection, attestation, data backup, and system maintenance, etc. This course will also introduce students to the various software resources that exist today to support TPMs, give a high-level overview of related research and development projects, and briefly discuss other trusted computing standards such as Trusted Network Connect, which may be relevant to enterprise deployment of TPMs and trusted computing.

Course Objectives:

- Understand both basic and advanced TPM capabilities, as well as other trusted computing standards and technologies
- Understand concepts of trusted computing, including variations created by the Trusted Computing Group, Microsoft, and Intel
- Apply trusted computing concepts to design simple applications
- Understand how TPMs and related technologies can be used in enterprise environments and for cutting-edge research
- Familiar technologies of data backup, maintenance and troubleshooting
- Know the necessary tools and information to design and build systems that take advantage of trusted computing
- The course includes a project.
- This course is 4.5 credits.

CSIS 512 – Cybersecurity Infrastructures (4.5 Q.crdts)

This course will provide a structured approach that can be followed step by step, so as to design and build enterprise security architecture and infrastructure that meets the needs of modern business. It is intensively practical but theoretical works and background are also covered in how to make cybersecurity work. The topics covered will include Introduction, Strategy and Planning (including financial budget and management), Enterprise Security Design, Implementation and Operations, and also the concept of ISO 27000:2013, the Information Security Management System (ISMS) framework, and NIST's SP800-30 publication about risk management.

Course Objectives:

- Understand and apply cybersecurity architecture principles
- Understand security domains, trust level, and tiered networks
- Understand the concepts of user awareness, guidance, administration, monitor, respond, & audit
- Develop strategy and planning (including financial budget and management, as well as contingency planning, etc.)
- Conduct risk assessments, set up monitoring systems and metrics based on the infrastructure and architecture
- Develop enterprise security policies, standards, and guidelines
- Understand what composes an information security team and their required experiences
- The course includes a project.
- This course is 4.5 credits.

CSIS 518 - Cryptography & Network Security (4.5 Q.crdts)

This course will provide a comprehensive overview of network security concepts and problems and the mechanisms and tools to secure networks. It will focus on the Internet, discuss the threats to and from the Internet and examine existing Internet security techniques and protocols and their limitations. Topics also include secret key and public key cryptography, Hash algorithms, authentication, IPSEC/VPN, IPSEC key exchange, SSL/TLS, firewall, anonymous communication, and VoIP security.

The design and analysis of security protocols and different attacks and defenses against them will be discussed within the course. Related topics about this include: signature and authentication protocols; privacy; digital rights management; security protocols for wired, wireless and distributed networks; electronic voting; payment and micropayment protocols; anonymity; broadcast encryption and traitor tracing; quantum cryptography; and visual cryptography.

In the cryptography section, this course deals with conventional, symmetric encryption and the various methods of attacking it. It will cover the historical substitution and transposition ciphers and symmetric block ciphers as well, which will be illustrated by an explanation of DES (Data Encryption Standard). The additional conventional algorithms of triple DES, IDEA (International Data Encryption Algorithm), and RC5 are discussed.

Course Objectives:

- Understand the network security concepts and problems and the mechanisms and tools to secure networks
- Describe foundational principles of modern cryptography
- Discuss how cryptographic models relate to real-world security
- Describe common complexity assumptions for cryptography
- Deploy firewalls and data encryption to minimize threats
- Install security software, and monitor networks for security breaches
- Plan, coordinate and implement network security measures
- Maintain network hardware and software
- Analyze problems and monitor networks to ensure availability for system users
- Identify customer needs and use the information to design, interpret and evaluate network requirements
- Use cybersecurity measures to protect data and manage personnel conduct in relation to safeguarding data
- The course includes a project.
- This course is 4.5 credits.

CSIS 520 – Practices for Cybers Threats and Defense (4.5 Q.crdts)

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad damage to company reputations. This course is designed for defenders to develop a solid foundation of core strategies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. In this course, a series of scenarios of many attacks and swift detections and appropriate responses to any breach that does occur will be discussed. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Not only to prevent network attacks and protect critical data, it is increasing important for any organization to be able to detect attacks in a timely fashion. For this purpose, at the end of this course students will also understand the traffic that is flowing on networks, how to look for indications of an attack, and how to perform penetration testing and vulnerability analysis against organizations to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Through this course, students will gain the knowledge by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures and completing the security lifecycle.

Course Objectives:

- Understand how to prevent network attacks and protect critical data
- Understand PREVENT - DETECT - RESPONSE security strategy
- Understand the enterprise network traffic, attack indications, penetration testing and vulnerability analysis
- Develop a solid foundation of core strategies and practices to defend an enterprise
- How to perform the forensics and develop more effective and robust preventive and detective measures
- The course includes a project.
- This course is 4.5 credits.

CSIS 528 – Network Principles (4.5 Q.crdts)

This course provides students with the instruction necessary to install, configure, and troubleshoot a computer network. This course presents current networking standards, the OSI Model, various protocols and topologies, the interconnections between various hardware components, network operating systems, DNS, DHCP, TCP/IP, Ethernet, wired and wireless transmission, and security.

In this course, students will also study security issues in Information Technology and Networking. Students are introduced to practical solutions for identifying, assessing, and preventing external and internal threats to networks. Key components include authentication methods, communication security, infrastructure security, cryptography basics, and security implementation.

Course Objectives:

- Understand computer networks and their purpose
- Understand network media and data transmissions
- Explain network design and describe the various network topologies
- Discuss local area network architectures
- Discuss network protocols and network software
- Describe the features of Windows servers
- Describe the features of NetWare and Linux servers
- Describe the issues involved in managing a local area network
- Discuss wide area networks
- Discuss the Internet and its tools
- The course includes a project.
- This course is 4.5 credits.

CSIS 530 – System Assessment & Security Risk Analysis (4.5 Q.crdts)

This course is designed for students to learn to identify Threat, Risk and Vulnerability, as applied to enterprise IT systems. It incorporates the physical safeguards and policies necessary to meet the requirements for the protection of data in a fixed site. Students will conduct a Site Security Analysis of a given facility, based on skills and information learned in class. Gap Analysis, Gap Closure and Countermeasures will be discussed and documented, in an effort to counter identified Vulnerabilities.

In this course, students will also learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Course Objectives:

- Understand the elements of risk assessment and the data necessary for performing an effective risk assessment
- How to map an organization's business requirements to implement security controls
- Develop risk management models for implementing a deeper risk management program in their organization
- Demonstrate proper risk management and risk analysis technique and methodology
- Demonstrate vulnerability assessment and threat analysis techniques
- Plan vulnerability assessment, threat assessment and risk analysis projects as it relates to physical security
- Prepare and present business-based recommendations for expenditure of security funds
- Develop administrative policies and procedures required to administer a physical security requirement in a secure environment

- Develop plans that address facility access and the protection of structures and components that contain the automated information system and network equipment
- Develop a Physical Security awareness program
- Facilitate physical safeguards that meet established requirements for data storage
- Illustrate risk analysis and protection of telecommunication
- Demonstrate the requirements for a Physical Security Site Security Analysis
- The course includes a project.
- This course is 4.5 credits.

CSIS 536 – Computing Operation Systems (4.5 Q.crdts)

Operating systems are an essential part of any computer system. Operating systems vary significantly, but their fundamental principles remain the same. This course examines operating system design concepts, data structures and algorithms, and systems programming basics. In this course, students will be introduced to the concepts of operating systems, see how they manage resources such as memory, peripherals, and schedule CPU time, learn how to use the system call interface and how to create processes and synchronize them, learn how applications communicate, understand the memory hierarchy and see how virtual memory is managed, understand how files are managed and stored, and much more.

The topics to be covered include: computer and operating system structures; process and thread management; process synchronization and communication; memory management; virtual memory; file system; I/O subsystem and device management; and selected examples in networking, protection and security.

Course Objectives:

- Gain extensive knowledge on principles and modules of operating systems
- Understand key mechanisms in the design of operating systems modules
- Understand process management, concurrent processes and threads, memory management, virtual memory concepts, and deadlocks
- Compare performance of processor scheduling algorithms
- Produce algorithmic solutions to process synchronization problems
- Use modern operating system calls such as Linux process and synchronization libraries
- Practice with operating system concepts such as process management, synchronization, networked processes and file systems
- The course includes a project.
- This course is 4.5 credits.

CSIS 540 - Ethical Hacker Skills and Technologies (4.5 Q.crdts)

This course covers information related to Ethical Hacking. This course includes lessons where students will learn what Ethical Hacking is and how to use these skills to become a paid security professional. This course is a starting point for students to chart the course to a well paying and satisfying Cybersecurity career. This course will get students on the fast track to be relentlessly pursued by recruiters.

The demand for Ethical Hackers, Cybersecurity Engineers, Administrators, Consultants, Architects, Business Analysts, Project Managers, etc. is immense. Ethical Hacking is an attainable path to helping business protect their digital assets in the cloud and on-premise.

Course Objectives:

- Learn the basics of Ethical Hacking
- Introduction to Ethical Hacker subject matter
- Learn hacking techniques through multiple hands-on examples in this course

- Intend for IT beginners and IT professionals looking to make the move into the Cyber Security field. No programming experience or prior security knowledge is required.
- Understand networking and TCP/IP concepts, technologies and principles.
- Prepare students who is interested in a career in Cybersecurity
- Teach many professionals to plan for and address Cybersecurity issues on a daily basis using free open source software tools.
- This course is 4.5 credits.

CSIS 545 - Advanced Ethical Hacker Skills and Cybersecurity (4.5 Q.credits)

This course is an advanced course of Ethical Hacking Skills and Technologies. This course teaches students who already took CSIS 540 and would like to master advanced Ethical Hacking principles, technologies, hands-on skills and popular tools. This course will get students to be a senior ethical hacker and efficiently protect his/her organizations to be attacked by outside-hackers.

Course Objectives:

- Learn the Advanced of Ethical Hacking
- Learn advanced hacking techniques through multiple hands-on examples in this course
- Intend for IT professionals looking to make the move into senior Cybersecurity engineer level.
- Understand advanced Internetworking technologies and principles.
- Prepare students to CEH certification test to be a certified Ethical Hacker.
- Lead junior Ethical Hackers to be a leader of Cybersecurity Engineers and Information Assurance Specialist.

CSIS 560 - Mobile Computing (4.5 Q.credits)

This course is offered for those who are interested in understanding and building systems support mechanisms for mobile computing systems including client-server web/database/file systems, and mobile ad hoc and sensor networks for achieving the goal of anytime, anywhere computing in wireless mobile environments. The technologies involved to realize such a system will be covered, and the fundamental concepts of mobile computing will be introduced. These include mobility and service management, data management, routing in mobile ad hoc and sensor networks, and security issues for mobile systems. While mobile computing covers many topics, in this course our main focus will be on mobility, data and service management, and security issues in mobile computing environments. Students are expected to be familiar with basic concepts in Operating Systems and Networks in this class.

Topics to be covered include mobility and location management, data and resource management, mobile ad hoc and sensor networks, security for mobile and wireless computing, and paper presentation and discussion.

Course Objectives:

- Understand wireless communication technologies and the proliferation of portable computing devices
- Understand the characteristics and limitations of mobile hardware devices, including their user-interface modalities
- Methodologies to access mobile network services and resources, from anywhere at any time.
- Understand security issues for mobile computing
- The challenges faced to efficiently enable such access along with state-of-the-art solutions
- The course includes a project.

CSIS 570 – Enterprise Security Technologies (4,5 Q. Crdts)

This course is designed to give students the ability to use advanced security technologies to perform penetration testing and ethical hacking to identify vulnerabilities within a network or website and properly secure it from hackers.

CSIS 570 is the must-have course for every well-rounded security professional. In this course, students will learn proper planning, scoping and recon, then dive into advanced techniques for scanning, target exploitation, password attacks and wireless and web apps. Students will be exposed to comprehensive penetration testing and ethical hacking know-how and various real-world network penetration test scenarios. Students will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course and discover and exploit vulnerabilities in a realistic sample target organization.

Course Objectives:

- Understand how to secure and protect any network from hackers and loss of data
- How to do penetration testing and ethical hacking by building a virtual hacking environment, attacking wireless networks, routers, and websites, and breaking encryptions and passwords
- Hands-on skills to use the most powerful ethical hacking tools, including Nmap, Nessus, Metasploit, John the Ripper, Rainbow Tables, web application attack tools
- Hands-on skills to utilize built-in operating system tools on Windows and Linux in a weaponized fashion
- How to perform a detailed, end-to-end professional penetration test using the best methodologies in the industry
- The course includes a project.

CSIS 580 – Cybersecurity Intelligence/Counter Intelligence (4,5 Q. Crdts)

This course is designed to help students who will take the role of network defenders and incident responders to construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs); to fully analyze successful and unsuccessful intrusions by advanced attackers; to piece together intrusion campaigns, threat actors, and nation-state organizations; to manage, share, and receive intelligence on APT adversary groups; to generate intelligence from their own data sources and share it accordingly; to identify, extract, and leverage intelligence from APT intrusions; to expand upon existing intelligence to build profiles of adversary groups; and to leverage intelligence to better defend against and respond to future intrusions.

Through the collection, classification, and exploitation of knowledge about adversaries, students will be given the information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Accurate, timely, and detailed information can be used to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. This course will train students to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

Course Objectives:

- Understand the concepts of cybersecurity intelligence/counter intelligence
- How to construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- How to analyze successful and unsuccessful intrusions by advanced attackers
- How to generate intelligence from attacking and security data sources
- How to identify, extract, and leverage intelligence from APT intrusions
- How to detect, scope, and select resilient courses of action in response to any intrusions and data breaches
- The course includes a project.

CSIS 585 - Malware Analysis and Defense (4,5 Q. Crdts)

This course will explore malware analysis tools and techniques in depth. It will help students acquire the practical skills to examine malicious programs that target and infect Windows systems and other operating systems. This course will cover malware analysis, and students will learn to determine how malware operates, what functionality is built in and what attacker-controlled domains or Internet Protocol (IP) addresses it communicates with. Failing to understand the malware functionality threatens all remediation efforts. This course will provide an introduction to the tools and methodologies used to perform dynamic and static analysis on portable executable programs found on Windows systems as well.

As malware authors continue to improve in their efforts to prevent the reverse engineering of their tools, students must learn to combat sophisticated malware by studying anti-analysis techniques. Advanced topics related to combating malware defense mechanisms will be discussed in this course. Additional topics covered will include malware stealth techniques such as process injection and rootkit technology, along with tools and techniques to aid in their analysis. All concepts and material presented are reinforced with demonstrations, real-world case studies, follow-along exercises and student labs to allow students to practice what they have learned.

Course Objectives:

- Understand the primary types of malware
- How to create a safe malware analysis environment
- Malware analysis shortcuts and the malware analysis and reporting process
- Legal issues involving malware analysis and reverse engineering
- Methodology differences between static and dynamic analysis
- Binary, decimal, hexadecimal conversion, and code, compilers and compilation
- The tools used to identify obfuscation methods and the tools used by analysts to recover the "hidden" or obfuscated data
- How to perform dynamic analysis with virtual machines and monitoring tools to capture system, registry and network activity generated during malware analysis
- The course includes a project.

CSIS 590 –Cloud Computing (4,5 Q. Crdts)

Cloud Computing has emerged in recent years as a new paradigm for hosting and delivering services over the Internet. This course is designed to introduce the concepts of Cloud Computing as a new computing paradigm. The students will have an opportunity to explore Cloud Computing's various terminology, principles and applications. The course will expose students to different views of understanding Cloud Computing such as theoretical, technical and commercial aspects. A variety of real case studies and existing in market cloud-based tools will be identified and studied in order to provide students with a close overview of Cloud Computing applications.

This course provides a hands-on comprehensive study of Cloud concepts and capabilities across the various Cloud service models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Business Process as a Service (BPaaS). The course also covers the Cloud security model and associated challenges and delves into the implementation and support of High Performance Computing and Big Data support capabilities on the Cloud. Through hands-on assignments and projects, students will learn how to configure and program IaaS services. They will also learn how to develop Cloud-based software applications on top of various Cloud platforms, how to integrate application-level services built on heterogeneous Cloud platforms, and how to leverage SaaS and BPaaS solutions to build comprehensive end-to-end business solutions on the Cloud.

Course Objectives:

- Understand the fundamentals and essentials of Cloud Computing
- Understand various Cloud service models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Business Process as a Service (BPaaS)
- Understand the foundation of the Cloud computing so that students are able to start using and adopting Cloud Computing services and tools in their real-life scenariosExplore some important Cloud

Computing driven commercial systems such as GoogleApps, Microsoft Azure and Amazon Web Services and other businesses cloud applications

- The course includes a project.

CSIS 591 - Digital Forensics (4,5 Q. Crdts)

This course is a study of the techniques behind digital forensic investigations and evidence collection and will cover the fundamental steps of the traditional computer forensic methodology. By the completion of this course, you will be able to use tools to extract data from live memory and captured network packets, recover deleted files, identify unknown file types, and analyze log files and registry.

Objective: Students will be able to:

- Describe digital forensics and relate it to an investigative process.
- Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

CSIS 592 - Forensic Analysis and Risk Management (4,5 Q. Crdts)

This course is designed from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. It focuses on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur.

This course will cover the tools, technology, and processes required to integrate network evidence sources into investigations, with a focus on efficiency and effectiveness. It will encompass the skills of not only capturing suspicious data, but also the ability to discern unusual patterns hidden within seemingly normal network traffic. This course offers hands-on experience with real-world scenarios that will help take students' work to the next level. Real-world examples will be utilized throughout the course in conjunction with numerous hands-on exercises to provide field proven, practical Forensics Analysis skills.

Course Objectives:

- Demonstrate the use of various forensic tools.
- Conduct digital investigations from the initial recognition of an incident through the steps of evidence gathering, preservation, and analysis
- Analyze major components of the NTFS and EX2 file systems and associated forensic artifacts
- Discover latest trends in digital forensics including IoT, mobile, cloud, SSD, and virtual machine forensics
- Explore the rules, laws, policies, and procedures that affect digital forensics
- Prepare reports that describe the technical procedures used in forensic investigations
- This course is 4.5 credits.

CSIS 593 – Advanced Applied Digital Forensics (4,5 Q. Crdts)

This course will familiarize information technology professionals with the application of forensic science principles and practices to the collection, preservation, examination, analysis and presentation of digital evidence. The course will include selected topics from the legal, forensic, and information technology domains and utilize lecture, laboratory and written projects to illustrate these topics.

Objective: Students will be able to:

- Solid skills in forensic science.
- Have a good understanding of digital evidence examinations.
- Be able to articulate the steps of the forensic process as applied to digital evidence.
- Be able to draft a Standard Operating Procedure.
- Using common forensic tools to conduct digital forensic examinations.
- Recognize the application of digital forensics with respect to information security
- This course is 4.5 credits.

CSIS 594 – Legal and Ethical Aspects of Cybersecurity (4,5 Q. Crdts)

This course is designed to bridge the gap between the legal department and the IT department caused by new laws on privacy, e-discovery and data security. This course covers the laws of business, contracts, fraud, crime, IT security, liability and policy - all with a focus on electronically stored and transmitted records. It also teaches students how to prepare credible, defensible reports, whether for cyber-crimes, forensics, incident response, human resource issues or other investigations.

This course also provides training for students for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, and PCI-DSS. This will strengthen the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business. This course will strengthen students' abilities to help enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security. Some breaking stories ranging from Home Depot's legal and public statements about payment card breaches to the lawsuit by credit card issuers against Target's QSA and security vendor will be examined within the course.

Course Objectives:

- Understand, identify and articulate the legal issues in the information assurance field
- Understand compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, and PCI-DSS
- Analyze and interpret how relevant case and statutory law has been applied to legal problems in information assurance
- Formulate how proposed legislation can be applied to solve legal problems with information systems
- How to develop and implement the legal compliance standards and processes
- How to reduce risk in a world of vague laws on cyber-crime and technology compliance
- How to carry out investigations so that they will be judged as ethical and credible
- How to choose words for better legal results in policies, contracts, and incidents
- How to respond to information security, privacy and forensic challenges
- The course includes a project.
- This course is 4.5 credits.

CSIS 595 - Information System Auditing and Monitoring (4,5 Q. Crdts)

This course is designed to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit and real-time monitoring best practices, the students will have the opportunity to dive deep into the technical "how to" for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for continuous monitoring and automatic compliance validation will be given from real world examples.

The course contents will cover audit planning and techniques, more effective risk assessment for control specification, firewall and perimeter auditing, a proven six-step audit process, time-based auditing, effective network population auditing, how to perform useful vulnerability assessments, uncovering "Back Doors," building an audit toolkit, detailed router auditing, technical validation of network controls, web application auditing, and audit and real-time monitoring tools.

Course Objectives:

- Understanding IT audit risks and defining audit scope
- Internal control concepts and the role of computer control standards
- General controls protecting the IT environment
- Business process controls covering specific financial systems
- Communicating audit findings
- Real-time system monitoring and technologies
- The course includes a project.
- This course is 4.5 credits.

CSIS 620 – Information System Security Principles & Practices I (4,5 Q. Crdts)

In this course, students explore the first four of the eight domains of the (ISC)² Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) in information security as a framework to critically analyze security awareness issues and to evaluate best practices in implementing security systems within the enterprise.

The CISSP certification can give a person opportunities to advance their career in the cybersecurity profession. For many governmental agencies, the CISSP certification is mandatory for senior and management level positions. CISSPs are information assurance professionals who define the architecture, design, management and controls that assure the security of business environments.

Course Objectives:

- Security and Risk Management
- Asset Security
- Security Architecture Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security.

CSIS 626 - Information System Security Principles & Practices II (4,5 Q. Crdts)

This course is the second portion of CISSP principles and Practices, students explore the other four of the eight domains of the (ISC)² Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) in information security as a framework to critically analyze security awareness issues and to evaluate best practices in implementing security systems within the enterprise. After these two courses training, students should have ability to take and pass CISSP certification examination.

The CISSP certification can give a person opportunities to advance their career in the cybersecurity profession. For many governmental agencies, the CISSP certification is mandatory for senior and management level positions. CISSPs are information assurance professionals who define the architecture, design, management and controls that assure the security of business environments.

Course Objectives:

- Understanding remind first four domains
- Identity and Access ManagementAsset Security
- Security Assessment and Testing
- Security Operations
- Software Development Security

- This course is 4.5 credits.

CSIS 636 - Database System Management & Assurance (4,5 Q. Crdts)

This course provides a managerial understanding and approach to the technical subject of database management. The course will illustrate the important role that database systems play in an organization and provide students with a background to understand the subject, and a foundation upon which to build management decisions. This course is designed to investigate how database management system techniques are used to design, develop, implement and maintain modern database applications in organizations.

Upon completion of this course, the student will be able to define essential database vocabulary, effectively apply data relationships and normalization techniques, describe the transformation of database design from a conceptual user model (e.g., an ERD) to a normalized relational model, explain and apply Structured Query Language (SQL) in a database environment, describe the methods available for minimizing DBMS risks and security failures, characterize the roles and responsibilities of the Database Administrator (DBA), and apply fundamental database concepts to an information systems problem.

Course Objectives:

- Understand the concepts of RDBMS
- Understand solid theoretical foundation in relational database technology
- Create basic data and process models
- Create a basic relational database model based on the data and process models
- Understand and discuss the concepts and principals of database security
- Understand the concepts and principals of personal privacy relative to database systems
- The course includes a project.
- This course is 4.5 credits.

CSIS 650 – System Architect and Cybersecurity (4,5 Q. Crdts)

This course covers the issues in designing and engineering large enterprise software systems. Technologies such as Web Services and Cloud Computing provide platforms for building such systems, and architectures such as service-oriented architecture (SOA), event-driven architecture (EDA) and representational state transfer (REST) are idioms for structuring such systems.

This course will focus on the development of high-assurance software systems via the secure system development life cycle process. This course will foster the design and implementation as well as verification/validation of secure software systems and architectures. A key coverage area will include principles and practices of secure and high assurance software development processes, including security development lifecycle models, and design/verification/validation using languages and tools such as UML. Tools and techniques for code analysis and testing, and evaluation and certification of software will also be emphasized. The course will also cover secure programming principles using different languages, with particular focus in secure software development.

Key topics within this course include secure development methodologies/models; assurance techniques (certification, validation, etc.); secure programming issues/practices and tools; software assurance and Security analysis - tools and techniques; secure design, testing and systems security engineering (e.g., protocol verification, model-based techniques, etc.); and supply chain security, life-cycle security, security risk analysis.

Course Objectives:

- Understand the principles and methodologies for designing and implementing secure systems and establishing software assurance
- Understand and analyze code for vulnerabilities and learn secure programming practices
- Use of tools for code analysis and security property verifications
- Apply secure design principles to build a real system
- The course includes a project.

- This course is 4.5 credits.

CSIS 665 – Disaster Recovery & High Availability (4,5 Q. Crdts)

Knowledge of Disaster Recovery and Business Continuity provides a strategic imperative and a competitive advantage in an environment where students must plan for the unexpected, maintain operations, and meet regulatory demands. This course covers recovery time and recovery point objectives (RTO and RPO). Built upon the concepts of risk analysis and business impact planning, this course is designed to provide a foundation and guide to coordinated organizational emergency response and event management during and after a disruptive occurrence.

This course begins by examining in depth the events of the past 20 years, including the lessons learned about the interdependencies of the critical infrastructures following the Oklahoma City bombing and the terrorist attacks against the World Trade Center and what we learned in the aftermath of hurricanes Katrina and Rita in the summer of 2005. While there are many cross-sector interdependencies to consider, this course will focus on the dependence of the various infrastructure sectors on the Internet, business continuity, and the impact of highly complex computer controlled systems. This course will also give the student a full examination of the scope of critical infrastructure vulnerabilities; the dependence of critical infrastructures on the Internet, and Internet security problems; elementary concepts of business continuity; high availability architecture; system design and solution roadmap; data center design and disaster recovery; and data center operations. The subject material requires at least a working knowledge of computer networks and business decision making.

Course Objectives:

- Understand the concepts of business continuity, high availability (HA) and disaster recovery (DR)
- Identify the core pieces and functions of an integrated, effective, corporate business continuity program
- Develop plans for Business Continuity/Disaster Recovery and Incident Response.
- Describe key Business Continuity terms and concepts, such as determining critical business functions, the "MARC" (minimum acceptable recovery configuration), Recovery Time Objectives, Recovery Point Objectives, Recovery Time Capabilities, information technology disaster recovery technical solution designs standards and practices
- Understand how to effectively determine business unit resumption requirements for loss of workspace, loss of information technology, and loss of personnel.
- Understand how to approach crafting effective information technology recovery time capabilities for key systems that will meet business units' stated needs, and how to address "the gap" which may be discovered between business units' information technology recovery requirements and available money or capabilities
- Understand the core quality control concepts surrounding the development and use of scorecards in evaluating business resumption and disaster recovery plans, and standardized objective metrics in information technology testing
- The course includes a project.
- This course is 4.5 credits.

CSIS 630 – Independent Project Study in Cybersecurity (4,5 Q. Crdts)

Approval by faculty member and program director is required prior to registration. Students will gain real-world industrial experience in the Cybersecurity field.

Prerequisites: Admission to the MS in Cybersecurity

CSIS 690 - Cybersecurity Capstone Project

The capstone is an opportunity for the student to demonstrate the Cyber Security skills gained throughout the program. The student will learn how to apply the tools, techniques, and knowledge gained throughout the

program in a practical, real-world setting. The goal for this course is to evaluate the knowledge and skills gained by students in the Cyber Security program.

CSIS 690 is the capstone course for the cyber security degree program which provides the student with a hands-on environment to test and apply knowledge and skills learned throughout the program. The student will be required to critically think through real-world scenarios and recognize the value of cyber security methodologies.

The course should be taken on the last term of the student's program. The 10-weeks-long capstone project is to provide students the opportunity to work with a faculty or industry mentor on a cybersecurity field. After completing the capstone Project, the student is expected to submit a Project presentation to demonstrate their mastery by gaining some useful technology or hands-on skills that will help their career development in Cybersecurity field.

Course Objectives:

- Understand capstone project, learning objectives, course requirements, goal of being achievement, and grade policy, etc.
- Solidify knowledge gained from the courses that make up the MS in Cybersecurity program.
- Demonstrate critical thinking and problem-solving skills on issues related to cybersecurity.
- Explain current policies and practices related to threats against information systems and infrastructures.
- Examine legal, social, and ethical concerns related to securing information systems and networks.
- Understand the differences between internal and external threats and how to defend against each.
- Discuss the important principles and theories that are used within the cybersecurity field.
- Demonstrate knowledge and hands-on skills in the field of cybersecurity to propose solutions for real-world problems.