Formed in 1990, the Norfolk State University Department of Computer Science was designed to provide students with fundamental training in the theoretical and practical aspects of computer science and information technology. The department offers a general computer science degree and options in Information Assurance, Information Systems and Computer Engineering. This wide range of options gives students the opportunity to pursue studies in Cybersecurity, Robotics, Software Engineering, Computer Networking, Web Design and Development.

The B.S. degree in Computer Science at Norfolk State University is accredited by the Computing Accreditation Commission of ABET. The Computing Accreditation Commission of ABET 415 N. Charles Street Baltimore, Maryland 21201 (410) 347-7700 http://www.abet.org

The Department of Computer Science offers the B.S. Degree in Computer Science, which includes the following specialty areas:

- Computer Science (General Program)
- Computer Engineering
- Information Systems
- Information Assurance

The program addresses a number of career opportunities within the curriculum. The Computer Engineering option is suitable for students who are interested in the design and implementation of hardware. The Information Systems option qualifies students for employment in business environments. The Information Assurance option is suitable for students who have an interest in securing the nation’s critical infrastructure from terrorists, hackers, criminals and other individuals intending harm against the nation and its people.

The Department of Computer Science also offers the B.S. degree in Information Technology. The BSITE program aims to provide graduates with the skills and knowledge to take on appropriate professional positions in information technology upon graduation and grow into leadership positions or pursue research or graduate studies in the field. This option is suitable for students who are interested in information technology applications especially networking, web design and development.

The Department of Computer Science offers two graduate programs: a Master of Science Degree in Computer Science and a Master of Science Degree in Cybersecurity. The Master of Science degree in Computer Science was initiated in August 2003.

This degree program has a general computer science concentration as well as concentrations in information assurance and communication networks. The Master of Science degree in Cybersecurity was started in 2015. The purpose this program is to produce professionals who will manage, maintain, and integrate cybersecurity in organization settings. The M.S. in Cybersecurity is designed to focus on computer security and to increase the pool of well-educated security professionals. Theory and practical training will be combined with critical thinking and communication skills that are required by professionals in the cybersecurity field. Students will be prepared to apply their knowledge to defend against cyber threats directed toward the USA. In addition, students will be prepared to provide needed cybersecurity services to US agencies and organizations. Students will not only be trained to defend against cybersecurity attacks but also to use digital forensics to identify attackers.

**Computer Science Programs**

- Computer Science, M.S. (https://catalog.nsu.edu/graduate/science-engineering-technology/computer-science/ms-computer-science/)
- Cybersecurity, M.S. (https://catalog.nsu.edu/graduate/science-engineering-technology/computer-science/ms-cybersecurity/)

**Computer Science Courses**

**Computer Science**

**CSC 521 Database Principles and Design (3 Credits)**
An introductory course emphasizing the basic concepts and principles of database systems. Topics include relational, hierarchical, and network approaches to data organization.

**CSC 526 Structured Programming (3 Credits)**
This is a one semester course that extensively covers programming concepts and techniques at an accelerated pace. Students learn how to develop, test, and debug programs on both Unix and Microsoft platforms. Topics covered include control structures, files, arrays, strings, classes and data abstractions, pointers, virtual functions, object-oriented concepts, linked lists, stacks, and queues.

**CSC 530 Data Communication (3 Credits)**
Focuses on the basic principles of computer communication as well as hardware and software designs. Topics include transmission media, data encoding, transmission techniques, protocols, switching networks, broadcast networks, and local area networks.

**CSC 535 Computer Security I (3 Credits)**
This course is designed for IT professionals to learn computer and network security theories and practices that can be used to significantly reduce the security vulnerability of computers on internal networks or the Internet. The course assumes some familiarity with various operating systems and computer networks. Topics include cryptography, program security, operating systems security, database security, network security, security administration, computer ethics, and legal issues.

**CSC 555 Management of Information Security (3 Credits)**
This course is designed for Security System Administrators and Managers responsible for the design, planning and management of security installations in business and government institutions. Topics include management of information security, security planning, security protection, best practices, risk management, operations security, legal issues and certification and accreditation. The course assumes some familiarity with various topics taught in an Introduction of Information Assurance course.

**CSC 564 Operating Systems (3 Credits)**
Topics include the history and evolution of operating systems, the concepts behind and structure of various operating systems, process scheduling, interprocess communication, input and output, multiprocessing, memory management, and file systems. Concepts of distributed operating systems are also introduced.
CSC 566 Advanced Computer Topics I (3 Credits)
Advanced computer topics not generally covered in the curriculum. Designed as a Computer Science elective – not as a replacement for any specific required course.

CSC 567 Advanced Computer Topics II (3 Credits)
Advanced computer topics not generally covered in the curriculum. Designed as a computer science elective – not as a replacement for any specific required course.

CSC 568 Advanced Computer Topics III (3 Credits)
Advanced computer topics not generally covered in the curriculum. Designed as a computer science elective – not as a replacement for any specific required course.

CSC 569 Artificial Intelligence (3 Credits)
In depth study of concepts and problem solving techniques of artificial intelligence. Topics include knowledge representation, functional and logic programming, machine learning, natural language understanding, computer vision, robotics, and societal impact.

CSC 570 Articial Intelligence (3 Credits)
Advanced computer topics not generally covered in the curriculum. Designed as a computer science elective – not as a replacement for any specific required course.

CSC 571 Game Design and Development (3 Credits)
This course introduces students to game design and development concepts. Topics include the history of games, genres, play elements, story and character development, game play and storyboard design, level and user interface design, and the game design document.

CSC 572 3D Game Programming (3 Credits)
This is a project-oriented course on 3D game, programming. Students will work in teams to design, implement and test-dimensional game with, interactivity, game state diagram, animation, sound, and constraints. Students will also learn the basics of graphic design and animation.

CSC 573 Principals of Modeling and Simulation (3 Credits)
This course introduces students to the major areas of simulation and the languages and systems used in these areas. Areas of simulation to be covered include gaming, military, health, network, business processes and transportation. The types of simulation software to be discussed include process oriented, discrete event oriented, general purpose, and simulation environments.

CSC 574 Advanced Computer Topics IV (3 Credits)
Advanced computer topics not generally covered in the curriculum. Designed as a Computer Science elective – not as a replacement for any specific required course.

CSC 575 3D Game Programming (3 Credits)
Designed to focus on interactive computer graphics hardware and software: display devices, 2D and 3D geometric transformations, raster algorithms, representation of curves and surfaces, hidden line removal and surfaces, shading algorithms, and color graphics.

CSC 576 Systems Programming (3 Credits)
Fundamentals of system and network programming methodology, techniques, system calls and library calls.

CSC 577 Compiler Construction (3 Credits)
An introduction to the fundamentals of compiler construction and language translation. Topics include lexical analysis, specifications of syntax, algorithms for syntactic analysis, code generation, and optimization techniques.

CSC 578 Machine Learning (3 Credits)
Machine learning is a subfield of artificial intelligence concerned with the design, analysis, implementation, and applications of programs that learn from experience. This course is about learning to extract statistical structure from data for making decisions, predictions, and visualizations. It gives in-depth coverage of advanced methods in machine learning, emphasizes approaches with practical relevance, and discusses a number of recent applications of machine learning.

CSC 579 Advanced Computer Architecture (3 Credits)
Principles and advanced topics of the instruction set architecture for uni-processors, embedded system processor, and multi-processor.

CSC 580 Digital Forensics (3 Credits)
Contact the department for specific course information.

CSC 581 Scientific Visualization (3 Credits)
Fundamental concepts of the algorithms and design principles underlying modern 3D computer graphics, data and scientific visualization.

CSC 582 Graduate Independent Study I (3 Credits)
Supervised independent project designed to give computer science graduate students an opportunity to explore a single topic in a one-to-one learning relationship with a faculty member.
CSC 697 Ethical Hacking and Penetration Testing (3 Credits)
Contact the department for specific course information

CSC 701 Continuing Registration (1-9 Credits)
A one credit hour course that allows students to maintain continuous registration status. Does not count towards the MS.CSC degree credits.

CSC 702 Practicum I (1 Credits)
A one credit-hour course that allows students to apply their skills in a work setting. The credit earned through this course will not be counted towards M.S.CSC degree credit. A student can take this course, and repeat it for up to three times, when he/she is away from campus on outside employment for internship or practical training in a related technical field. This is a Pass/Fail course.

CSC 703 Graduate Research (3-9 Credits)
This course is designed to give students an opportunity to conduct research through practical experience with a graduate research advisor. It gives students an opportunity to gain exposure to a subset of tasks such as development and implementation of a research topic, literature, writing status and technical reports or papers for conference submission, and attending and making technical presentations. Topics vary based on the student's research activities.

CSC 720 Wireless Sensor Networks (3 Credits)
An advanced, graduate-level course focusing on study of wireless sensor networks from communications, security, and computing platform viewpoints. Wireless sensor networks are a sensing, computing and communication infrastructure enabling the monitoring and manipulating of the environment.

CSC 730 Advanced Topics in Networking (3 Credits)
This course includes the major fields in optical networks, dynamic spectrum access in wireless networks, cognitive radio networks, network coding, and other newly emerged networking technologies. For optical networks, the topics include WDM network elements, routing and wavelength assignment algorithms, blocking probability analysis, virtual/network topology design, survivability, and IP over WDM. For dynamic spectrum access or cognitive radio networks, the topics include enabling technologies for cognitive radio, channel assignment/seizion, routing, security, and spectrum management. This course will also cover network coding and other new ideas.

CSC 745 Network Defense (3 Credits)
Focuses on network defense and countermeasures, including firewalls, intrusion detection and prevention systems, virtual private networks.

CSC 750 Evolutionary Computing (3 Credits)
The fundamentals of applying biological evolutionary characteristics to optimization of very complex problems.

CSC 755 Cloud Computing (3 Credits)
A one-semester graduate-level course focuses on cloud computing technologies and solutions. It is designed to give students a solid foundation in cloud computing fundamentals. The course covers both the conceptual and practical aspects of cloud computing.

CSC 760 Secure Software Development (3 Credits)
Introduction to basic concepts and the latest research trends and results in developing secure software. Topics include the best practices in developing secure software within Software Development Lifecycle (SDLC), vulnerability assessment, and code analysis techniques.

CSC 765 Advanced Topics in Information Assurance (3 Credits)
Survey of current topics in Information Assurance

CSC 781 Advanced Graduate Topics I (3 Credits)
Advanced computer topics not generally covered in the graduate 600/700 level curriculum. Designed as a Computer Science graduate elective – not as a replacement for any core course.

CSC 782 Advanced Graduate Computer Topics II (3 Credits)
Advanced computer topics not generally covered in the graduate 600/700 level curriculum. Designed as a Computer Science graduate elective – not as a replacement for any core course.

CSC 791 Graduate Independent Study II (3 Credits)
Supervised independent project designed to give computer science graduate students an opportunity to explore a single topic in a one-to-one learning relationship with a faculty member.

CSC 795 Masters Project (3 Credits)
First semester of the Master's Thesis sequence. Under the supervision of the thesis director, students prepare a thesis proposal and work toward the goal of completing all background material needed for their research. Minimally, a satisfactory thesis draft will be used to satisfy completion of the course. The Graduate Committee must approve the thesis topic.

CSC 798 Masters Thesis I (3 Credits)
First semester of the Master’s Thesis sequence. Under the supervision of the thesis advisor, students prepare a thesis proposal and work toward the goal of completing all background material needed for their research. Minimally, a satisfactory thesis draft will be used to satisfy completion of the course. The Graduate Committee must approve the thesis topic.

CSC 799 Masters Thesis II (3 Credits)
The culmination of the two semester master's thesis sequence. Students must complete the thesis and defend it to a committee.

Cybersecurity

CYS 564 Secure Operating Systems (3 Credits)
This course introduces students to Operating Systems with emphasis on security. Students will be introduced to the foundations of Operating Systems, the vulnerabilities of Operating Systems, threats from attackers, potential harm that can be caused by attacks, defense and risk mitigation. The notion of a trusted Operating System will be introduced as a standard useful for comparing various Operating Systems.

CYS 573 Network Fundamentals (3 Credits)
This course introduces students to the basics of networks and their functionality, including the Open Systems Interconnection model, network components, local and wide area networks, routers, switches, wireless communication, network security, Internet protocols, and network applications such as web and email. It also covers the fundamentals of configuring and troubleshooting network features on popular computing platforms.

CYS 672 Computer and Network Forensics (3 Credits)
This course introduces students to the fundamentals of digital forensics, including forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentation, and case studies. Students will apply information security practices and technologies in virtual lab environments to gain hands-on experience solving realistic cybersecurity problems.

CYS 688 Human Aspects of Cybersecurity (3 Credits)
This course focuses on the theory and practice of implementing secure database systems. Emphasis will be placed on database security principles, database application security models, database auditing models, security implementation and database reliability.
CYS 697 Ethical Hacking and Penetration Testing (3 Credits)
This course is designed for students pursuing a graduate degree in cybersecurity with particular interest in working as a white hat hacker. The students will be trained theoretically and practically in understanding vulnerabilities in network architectures, operating systems, database management systems and web servers. They will learn how exploits are designed by an adversary attacker to penetrate into vulnerable systems. The students will also learn how the hacker can move into a hacked system and remove her/his footprints. The course will expose students to a host of tools used for network scanning, fingerprinting and password cracking. These tools include Nmap, Nessus and Backtrack among others. There will be a thorough discussion on the emerging hack technology for wireless LANs and defenses against them.

CYS 721 Database Security (3 Credits)
This course focuses on the theory and practice of implementing secure database systems. Emphasis will be placed on database security principles, database application security models, database auditing models, security implementation and database reliability.

CYS 755 Healthcare Information Security (3 Credits)
This course is designed for students seeking to learn more about the field of healthcare information security. It covers the fundamentals of computer and network security theories and practices that can be used to significantly reduce the security vulnerability of healthcare information on internal networks or the Internet. An in-depth view of healthcare information is provided by examining healthcare regulatory requirements and the functions of a healthcare organization, including its medical business operations, hardware, software, networking, and security. Topics include electronic health records, security policy, web security, database security, security administration, and ethics, privacy, and law.

CYS 765 Advanced Topics in Cybersecurity (3 Credits)
This course covers state-of-the-art advances, emerging trends, and threats in cybersecurity. Topics to be covered include current topics in Information Assurance, advanced digital forensics, new approaches to management of cybersecurity and new threats, vulnerabilities, and controls.

CYS 795 Cybersecurity Capstone (6 Credits)
This project course is the capstone experience for graduate students in the Master’s degree in Cybersecurity. This course provides students with the opportunity to carry out in-depth research on a specified topic in cybersecurity. The student’s project will reflect the integration and application of the cybersecurity knowledge gained over the course of the program.

CYS 798 Cybersecurity Capstone I (3 Credits)
This course prepares students for their capstone experience in the Cybersecurity MS degree program. Capstone I provides the opportunity to carry out in-depth research on a specific topic in cybersecurity and career growth; to choose a specific topic in cybersecurity as the focus for their research; to identify a CYS faculty advisor who agrees to oversee their capstone project; and to develop a viable research proposal.

CYS 799 Cybersecurity Capstone II (3 Credits)
This course is the capstone experience for graduate students in the Master’s degree in Cybersecurity. Capstone provides students the opportunity to carry out in-depth research on a specific topic in cybersecurity under the guidance of a faculty research advisor. The student’s project will reflect the integration and application of cybersecurity knowledge and skills gained over the course of the program.

Faculty
Dr. Felicia Doswell, Associate Professor
Networks, security, privacy, internet technology, web performance evaluation, and game design.

Dr. Jonathan Graham Jr., Professor
Computational intelligence, digital forensics, smart intrusion detection systems, cybersecurity research, education and development.

Dr. Cheryl Hinds, Assistant Professor

Dr. Mary Ann Hoppa, Assistant Professor
Information visualization, metrics, microlearning, knowledge management, “hard problems” in cybersecurity, and wearable technology.

Dr. George Hsieh, Professor
Networking, network security, information assurance, communication systems and applications.

Dr. Yen-Hung Hu, Associate Professor
Network Security, Secure Programming, IT Compliance and Trustworthy Computing

Dr. Thorna Humphries, Associate Professor and Graduate Program Director
Software engineering, data management, computer science education, and security.

Dr. Samuel Olatunbosum, Associate Professor
Cybercrime and internet security, cloud computing efficiency, and societal impact of social networks.

Dr. Claude Turner, Associate Professor

Dr. Luay Wahsheh, Associate Professor
Computer security, information assurance, wireless network security, software security, and database security.

Dr. Aurelia T. Williams, Professor
Information assurance, computer forensics, network security, data communications, and computer science education.

For more information contact the Graduate Program Coordinator:
Dr. Thorna Humphries
Computer Science Department Norfolk State University
(757) 823-8318 voice | (757) 823-9229 fax
thumphries@nsu.edu | http://www.cs.nsu.edu