EC-COUNCIL UNIVERSITY

ACCREDITED. FLEXIBLE. ONLINE.

THE LEADER IN CYBER SECURITY EDUCATION

Catalog 2017

Effective: Jan 01- Dec 31, 2017

TABLE OF CONTENTS

A Message from the EC-Council University President

JAY BAVISI

President of EC-Council University

Cyber security leaders of tomorrow.

At EC-Council University, we have high aspirations for our students. They will be tomorrow's technology leaders. We strive to prepare our graduates to embrace the challenging position of Cyber security Specialists in International organizations worldwide. We consider this to be the school where chief cyber security officers and e-business architects of world class stature are educated.

We have built this institution on four main principles. First, we understand the Technology Revolution and aim to prepare our students to excel in the new future. Second, we embrace a new learning paradigm where knowledge is shared across space, time, and medium using our Learn Anywhere Anytime model. Third, we provide course content and materials that are highly relevant and fresh out of many research and development labs. Finally, we believe in a professional faculty who openly share their experience and knowledge with our students.

It is these principles and a strong sense of mission that drives all my colleagues and associates of EC-Council University to provide not only the most high-tech content and learning resources, but also a learning system and environment which allows every student at EC-Council University to learn, experience, and lead into the digital age with confidence.

Jay Bavisi
President of EC-Council University

THE UNIVERSITY

Mission Statement

Through **quality** distance educational programs, **excellence** in teaching and research, and direct connections to the cyber security industry, EC-Council University aspires to be an educational **leader** in cyber security . Our **students** of today will become the cyber security leaders of tomorrow.

University History

EC-Council University was incorporated in Wyoming in 2003 and licensed by the New Mexico Higher Education Department in 2006. The institution was created to educate and train cyber security professionals. Cyber security involves in-depth knowledge of a wide array of hardware and software systems as well as the skills and techniques to negotiate them. EC-Council, a world leader and creator of cyber-security certifications used throughout the globe and is the parent company of EC-Council University. EC-Council University President Sanjay Bavisi believes that cyber security professionals must not only have skills and techniques, but they must be educated to step into leadership and managerial roles in their companies, agencies, and organizations. This belief led to the establishment of the Master of Science in Cyber Security program.

Institutional Values

ECCU places particular value on the qualities of ethical behavior, innovative thinking, critical thinking, leadership, and the students. In a field as narrow and yet far-reaching as cyber security, these values promote and advance the ultimate goal of educating cyber security experts prepared to make the world safer and more secure for everyone. By incorporating these values with our course content and assessment measures, the educational environment becomes a dynamic and multi-dimensional process that empowers our students to become critical and innovative thinkers as well as, research-oriented problem solvers who embody high ethical standards, leadership skills, and an understanding of the global impact of their work.

Licensure

EC-Council University is licensed by the New Mexico Higher Education Department at 2048 Galisteo Street, Santa Fe, New Mexico, USA, 87505-2100, 505-476-8400; The Indiana Commission for Higher Education, Indiana Board for Proprietary Education, 101 W. Ohio Street Ste 670, Indianapolis, IN 46204-1984

CNSS Standards

ECCU courseware for ECCU 500, 501, 502, 503, 506 and 513 mapped to the former Committee on National Security Standards (CNSS).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort including more than 20 federal departments and agencies, academia, and industry. The goals of this initiative are to: 1) maintain a globally-competitive cybersecurity workforce; and, 2) broaden the pool of skilled workers able to support a cyber-secure nation.

One of the most important aspects of cybersecurity workforce planning is identifying the workforce and numerous workload requirements that impact the nature of the work performed. The Cybersecurity Workforce Framework provides a systematic way for educators, students, employers, employees, training providers, and policymakers to organize the way they think and talk about cybersecurity work and workforce requirements.

ECCU courseware for CIS 300, CIS301, CIS302, CIS303, CIS304, CIS308, CIS401, CIS402, CIS403, CIS404, CIS405, CIS406, CIS407,and CIS408 have been mapped to the National Initiative for Cybersecurity Education (NICE) framework. Also, the courses are mapped to the Center For Academic Excellence (CAE) knowledge, skills and abilities (KSA).

Contact Information

HOURS OF OPERATION
Monday - Friday 8am - 4pm MST

ECCU LOCATION/MAILING ADDRESS:

EC-Council University 101 C Sun Ave NE Albuquerque, NM 87109

info@eccu.edu
www.eccu.edu

Tel: 1-505-922-2889
Fax: 1-505-856-8267

Accreditation

EC-Council University is accredited by Distance Education Accrediting Commission (DEAC).

The Distance Education Accrediting Commission (DEAC) is a private, nonprofit organization founded in 1926 that operates as a national accreditor of distance education institutions.

Accreditation by DEAC covers all distance education activities within an institution and it provides a single source of nationally recognized accreditation from the secondary school level through professional doctoral degree granting institutions.

*The Distance Education Accrediting Commission is listed by the U.S. Department of Education as a nationally recognized accrediting agency.

*The Distance Education Accrediting Commission is a recognized member of the Council for Higher Education Accreditation."

CHEA
Accredited by a CHEA-recognized accrediting organization

DEAC
DISTANCE EDUCATION ACCREDITING COMMISSION

INSTITUTIONAL GOALS AND OBJECTIVES

Strive to strengthen Institutional effectiveness and collegial governance.

- Promoting and encouraging continuous learning and support
- Fostering collaboration amongst University administration and faculty
- Maintaining a high level of integrity

Ensure excellence in cyber security

- Providing high quality Cyber Security programs that meet the evolving needs of Cyber Security
- Retaining an up-to-date database of advanced Cyber Security articles and textbooks
- Ongoing research and development for quality improvements

Develop an engaged, diverse, high-quality student population while increasing student learning

- Encouraging student to student threaded discussions
- Online implementation of iLabs for student engagement
- Promoting cyber security educational programs and webinar's at no cost to the public
- Preparing our students to be socially responsible in Cyber Security leadership roles

Provide a supportive and welcoming environment to a diverse academic community

- Faculty and ECCU administration will serve as role models of socially responsible leaders
- Employees will demonstrate core values in the work place
- Maintaining qualified university staff and faculty

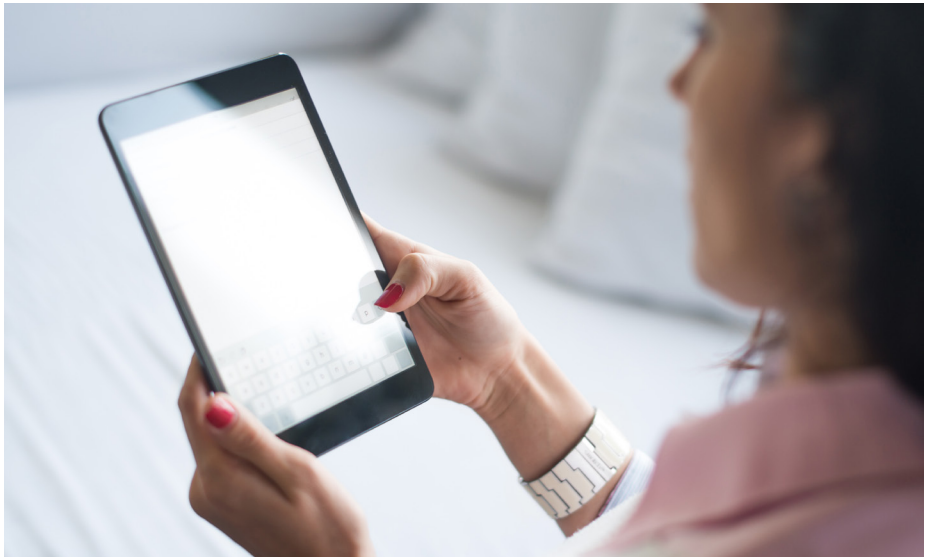
EC-COUNCIL UNIVERSITY 2017 ACADEMIC CALENDAR

Dates and Deadlines

	Term Start Date	Term End Date	Registration Begins	Registration Ends	Payment Deadline	Last day to withdrawal with a W	Last day to withdrawal from classes
Term 1	January 3, 2017	March 26, 2017	November 28, 2016	December 15, 2016	December 15, 2016	January 9, 2017	February 27, 2017
Term 2	April 3, 2017	June 25, 2017	March 6, 2017	March 30, 2017	March 30, 2017	April 10, 2017	May 29, 2017
Term 3	July 3, 2017	September 24, 2017	June 5, 2017	June 29, 2017	June 29, 2017	July 10, 2017	August 28, 2017
Term 4	October 2, 2017	December 20, 2017	September 4, 2017	September 29, 2016	September 28, 2017	October 9, 2017	November 27, 2017

2017 Holidays

New Year's Day	January 2 - Closed
Martin Luther King Jr. Day	January 16th - Closed
Presidents Day	February 20th - Closed
Memorial Day	May 29th - Closed
Independence Day	July 4th - Closed
Labor Day	September 4th - Closed
Columbus Day	October 9th - Closed
Th anksgiving Day	November 23rd - 24th - Closed
Winter Break	December 23rd - January 1st - Closed



2017 COURSE OFFERING

Bachelor's Program

Course Number	Page Reference	Course Title for Bachelor 2017 - Term 1 January 3, 2017
CIS 300	pg 22	Fundamentals of Information Systems Security **CSCU - Certifi ed Secure Computer User**
CIS 304	pg 23	Auditing IT Infrastructures for Compliance
CIS 405	pg 26	Internet Security: How to Defend Against Attackers on the Web
CIS 408	pg 27	Wireless and Mobile Device Security

Course Number	Page Reference	Course Title for Bachelor 2017 - Term 2 April 3, 2017
CIS 301	pg 22	Legal Issues in Information Security
CIS 308	pg 24	Access Control, Authentication and Public Key Infrastructure
CIS 402	pg 25	Security Strategies in Linux Platforms and Applications
CIS 406	pg 27	System Forensics, Investigation and Response **CHFI - Computer Hacking Forensic Investigator**
COM 340	pg 29	Communication and Technical Writing (ENG 340)

Course Number	Page Reference	Course Title for Bachelor 2017 - Term 3 July 3, 2017
CIS 300	pg 22	Fundamentals of Information Systems Security **CSCU - Certifi ed Secure Computer User**
CIS 304	pg 23	Auditing IT Infrastructures for Compliance
CIS 405	pg 26	Internet Security: How to Defend Against Attackers on the Web
CIS 408	pg 27	Wireless and Mobile Device Security

Course Number	Page Reference	Course Title for Bachelor 2017 - Term 4 Oct 2, 2017
CIS 301	pg 22	Legal Issues in Information Security
CIS 303	pg 23	Security Policies and Implementation Issues
CIS 401	pg 24	Security Strategies in Windows Platforms and Applications
CIS 404	pg 26	Hackers Techniques, Tools and Incident Handling **CEH - Certifi ed Ethical Hacking**
COM 340	pg 29	Communication and Technical Writing (ENG 340)
BIS 430	pg 30	Ethics for the Business Professional

Master's program

Course Number	Page Reference	Course Title for Master 2017 - Term 1 January 3, 2017
ECCU 501	pg 34	Ethical Hacking and Countermeasures **CEH - Certifi ed Ethical Hacking**
ECCU 502	pg 35	Investigating Network Intrusions and Computer Forensics **CHFI - Computer Hacking Forensic Investigator**
ECCU505	pg 37	Introduction to Research and Writing for the IT Practitioner
ECCU 512	pg 40	Beyond Business Continuity: Managing Organizational Change
ECCU 519	pg 44	Capstone
MGT 450	pg	Project Management

Course Number	Page Reference	Course Title for Master 2017 - Term 2 April 3, 2017
ECCU 500	pg 34	Managing Secure Network Systems
ECCU 504	pg 36	Foundations of Organizational Behavior for the IT Practitioner
ECCU 505	pg 37	Introduction to Research and Writing for the IT Practitioner
ECCU 514	pg 41	Quantum Leadership
ECCU 515	pg 42	Project Management in IT Security
ECCU 517	pg 43	Cyber Law

Course Number	Page Reference	Course Title for Master 2017 - Term 3 July 3, 2017
ECCU 501	pg 34	Ethical Hacking and Countermeasures **CEH - Certifi ed Ethical Hacking**
ECCU 502	pg 35	Investigating Network Intrusions and Computer Forensics **CHFI - Computer Hacking Forensic Investigator**
ECCU 505	pg 37	Introduction to Research and Writing for the IT Practitioner
ECCU 512	pg 40	Beyond Business Continuity: Managing Organizational Change
ECCU 519	pg 44	Capstone

Course Number	Page Reference	Course Title for Master 2017 - Term 4 Oct 2, 2017
ECCU 500	pg 34	Managing Secure Network Systems
ECCU 503	pg 36	Security Analysis and Vulnerability Assessment
ECCU 505	pg 37	Introduction to Research and Writing for the IT Practitioner
ECCU 509	pg 38	Securing Wireless Networks
ECCU 510	pg 39	Secure Programing

* Has a $50 lab fee

Courses offerings are subject to change to meet the needs of students and the University.

Application Procedure

Submit the following documentation for a complete application for admission:

All admissions applications are online http://www.eccu.edu/student-services/admission/. or you may contact: info@eccu.edu to be emailed a link to the admission application.

1. Complete the online admissions form. including all requested documents and application fee.
2. Request official transcripts from prior schools or NACES or NAFSA evaluation (for international degrees) be sent to :
   ATTN: Admissions
   EC-Council University
   101 C Sun Ave NE, Albuquerque, NM 87109

Applicants with a degree from a non-US institution

Applicants must provide proof of the US equivalency of your foreign degree. In order to have your degree from a non-US institution evaluated, you must submit unofficial transcripts for all degrees earned to either a NACES or NAFSA evaluator. The transcripts must include a list of all classes completed and grades awarded.

For international transcripts you will need to obtain a NACES or NAFSA evaluation. You will need to contact the University where you earned your bachelor's degree and request that they send your official transcript and other official documentation as requested by the evaluating agency. For NACES: A list of evaluators can be found on the NACES website http://www.naces.org/members.html. The evaluator must send the results of the evaluation directly to ECCU. For NAFSA: All documents must be sent to ECCU, and the student pays the evaluation fee online. For both NACES and NAFSA evaluations, all documents written and issued in a foreign language must have a certified English translation attached.

Official evaluations must be sent to:
ATTN: Admissions
EC-Council University
101 C Sun Ave NE, Albuquerque, NM 87109, USA

1. If our evaluator cannot evaluate your transcript you must have the transcript evaluated by an evaluator who is a member of NACES. You must choose an evaluator who is listed as a member of NACES to complete the evaluation. A list of evaluators can be found on the NACES website http://www.naces.org/members.html. The evaluator must send the results of the evaluation directly to ECCU.

   Official evaluation results must be sent directly to:
   ATTN: Registrar
   EC-Council University
   101 C Sun Ave NE, Albuquerque, NM 87109, USA

English requirement for international students

There are several ways to show Proof that you meet the English Requirement.

1. If your degree is earned in a country where English is the official language then you do not need to provide additional proof. For example, if your degree was earned in the UK, Canada, Australia, Ireland, New Zealand, or Nigeria.

2. If English was the Language of Instruction at the University where you earned your bachelor's degree then you can provide a letter from the institution stating that English was the language of instruction, and/or you can also request that the NACES or NAFSA evaluator state the language of instruction on the degree evaluation.

Here is a list of countries where Higher Education is commonly conducted in English:

Anguilla, Antigua and Barbuda, Bahamas, Barbados, Belize, Bermuda, Botswana, British Virgin Islands, Cameroon, Cayman Islands, Dominica, Fiji, Gambia, Ghana, Gibraltar, Grenada, Guyana, Jamaica, Kenya, Lesotho, Liberia, Malawi, Malta, Mauritius, Montserrat, Namibia, New Zealand, Papua New Guinea, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Swaziland, Tanzania, Tonga, Trinidad and Tobago, Turks and Caicos Islands, Uganda, Vanuatu, Zambia and Zimbabwe.

3. You can show English Proficiency by taking a recognized English proficiently test.
    a. Official TOEFL PBT (Test of English as a Foreign Language Paper-Based Test) score of 550 or better;
    b. OR Official TOEFL IBT (Test of English as a Foreign Language Internet-Based Test) score of 71 or better;
    c. OR Official IELTS (International English Language Test) score of 6.5 or better.

Technology Requirements

To succeed in our program, you must have the following technology capabilities:

Personal Computer
with Windows Operating System

Internet Connection
Access to (for proctored exams):

Webcam

Microphone

International Student Admission and Visa Services

The University does not provide any immigration status sponsorship or any type of student visa (INS Form I-20). Students who have obtained student visas, while attending other American colleges or universities in the United States, cannot maintain their student visa status based on enrollment at EC-Council University.

Student Enrollment Agreement

After the student is admitted to ECCU, they will receive a Student Enrollment Agreement which sets out the rights, responsibilities, tuition/ refunds and expectations of the student and the University. Registration for the first term is included in the enrollment agreement. After the student returns the signed enrollment agreement, they will be issues a login for MyECCU. An example student enrollment agreement may be found on the website at: www.eccu.edu

Academic Services

Students enrolled in the institution have access to academic consultation services. Students are able to interact with academic advisors via telephone, e-mail, printed materials, and other forms of communication. Additionally, instructors have virtual office hours during which time they will answer questions and concerns of individual students. ECCU administrators are available Monday- Friday 8am-4pm MST, and by email outside regular business hours. Instructor virtual office hours are posted on the course syllabus.

Students have access to individual sources of information about non-academic and other matters via the student portal. Students will be informed about whom to contact regarding specific types of questions or concerns. In addition, students have access to the online library.

Admission Requirements

Bachelor's Program

Applicants must:

- Be at least 18 years old prior to the beginning of requested term
- Have earned an associate's degree or foreign equivalent from an appropriately accredited institution that is listed in the International Handbook of Universities, accredited by an agency recognized by the US Secretary of Education, and/or the Council for Higher Education Accreditation (CHEA)

  OR have completed 60+ semester credit hours (90+ quarter credit hours) or foreign equivalent from an appropriately accredited institution that is listed in the International Handbook of Universities, accredited by an agency recognized by the US Secretary of Education, and/or the Council for Higher Education Accreditation (CHEA)

  AND Must submit proof of High School Diploma or foreign equivalent.

- Have a cumulative grade point average (CGPA) of 2.0
- Have completed a college level English and Math class with a grade of C or higher.
- Be sufficiently proficient in English - - one of the following must be met for international degrees:
  - TOEFL (Test of English as a Foreign Language Paper Based Test): 500 or higher
  - IBT (Test of English as a Foreign Language Internet-Based Test): 61 or higher
  - IELTS (International English Language Test): 6.0 or higher
  - Official transcript indicating completion of at least 30 semester hours of credit with an average grade of B or higher at an appropriately accredited college or university where the language of instruction was English

Master's and Graduate Certificate Programs

Applicants must:

- Be at least 18 years old prior to the beginning of requested term
- Have earned their bachelor's degree or foreign equivalent from an appropriately accredited institution that is listed in the International Handbook of Universities, accredited by an agency recognized by the US Secretary of Education, and/or the Council for Higher Education Accreditation (CHEA)
- Have a cumulative grade point average (CGPA) of 2.5
- Be sufficiently proficient in English - one of the following must be met for international degrees:
    - TOEFL (Test of English as a Foreign Language Paper Based Test): 550 or higher
    - IBT (Test of English as a Foreign Language Internet-Based Test): 71or higher
    - IELTS (International English Language Test): 6.5 or higher
    - Official transcript indicating completion of at least 30 semester hours of credit with an average grade of B or higher from an appropriately accredited college or university where the language of instruction was English

Applicants who are denied admission can appeal the decision to the Dean.

TRANSFERRING CREDIT

Course Transfer Credits

EC-Council University accepts college-level courses for consideration of transfer from accredited US or foreign equivalent institutions on a case by case basis. Computer technology courses (including cybersecurity academic credits) must have been earned within the last 15 years for consideration. Credits must be from institutions accredited by an agency recognized by the US Secretary of Education and/or the Council for Higher Education Accreditation (CHEA), or an accepted foreign equivalent that is listed in the International Handbook of Universities. The classes must closely correspond with EC-Council University courses and the student must have earned a grade of "B" or higher.

To begin the process, submit an official transcript or NACES/NAFSA evaluation. ECCU will evaluate all transcripts for potential transfer credit. The transfer credit must come from classes equivalent to the same level of education and learning outcomes as the degree coursework.

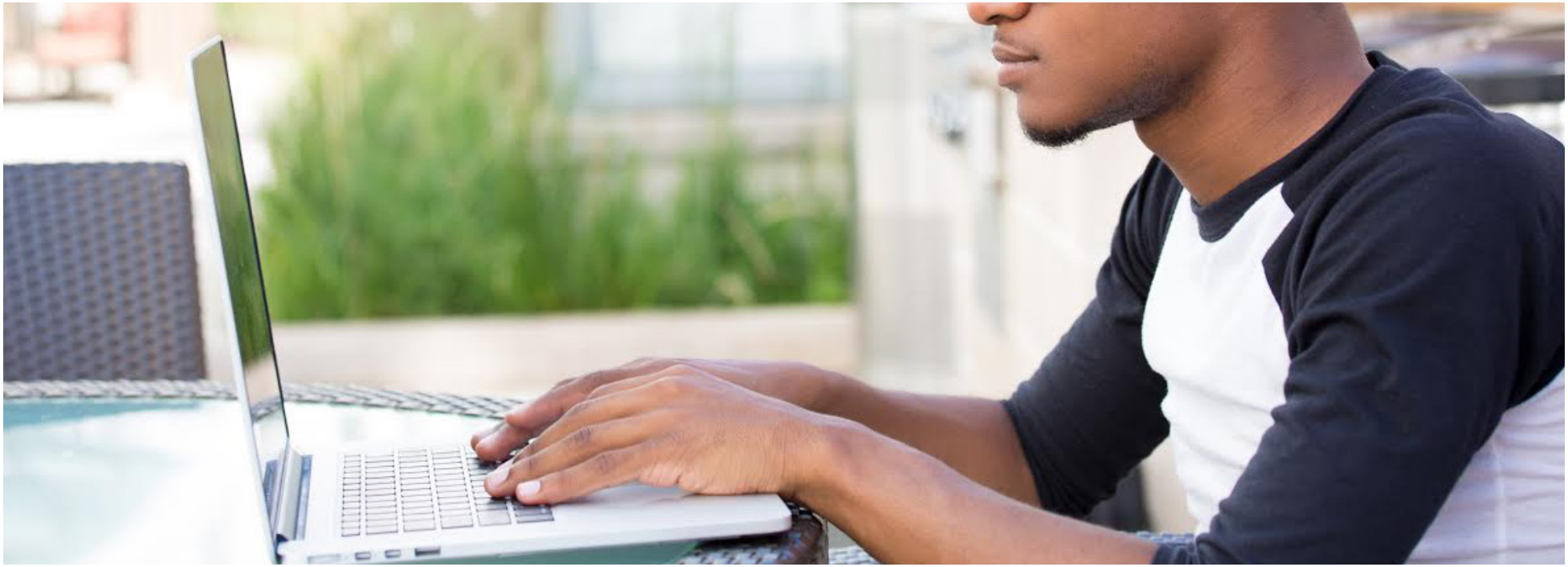
Students may receive a maximum of 18 graduate credit hours of transfer credit in the graduate program and 90 credits of transfer credit in the Bachelor's program. . Transfer credits are not considered in the calculation of the student's ECCU cumulative GPA.

Prior Learning Portfolio

As a prospective EC-Council University student, you may be awarded appropriate credit for your demonstrated knowledge gained from experiential learning. This learning may result from an industry certification, in-service training, and/or employment experiences.

To request credit based on experiential learning, you are required to provide documentation of the learning experience (certificates, employment records) and demonstrate acquired knowledge, skills, and competencies linked to the learning outcomes for the course(s) for which you are seeking credit. Credit for experiential learning is awarded based on a portfolio assessment by ECCU administrative team.

A Prior Learning Portfolio template is available for you to use in our website at http://www.eccu.edu/wp-content/uploads/2015/06/Prior-Learning-Portfolio-Template-fillable.pdf. Submit your portfolio and all supporting documents to registrar@eccu.edu. Within 5 business days you will be notified of what, if any, credit you will receive and how it will apply to your degree plan.



Maximum Allowable Transfer Credit

Students may receive a maximum of 9 graduate credits and 30 hours of undergraduate credit of transfer certification credits as evaluated using the Prior Learning Portfolio, from the Prior Learning Assessment. The limit for total award of transfer credit, including both credit awarded for courses from other Universities and credit awarded from the prior learning portfolio may not exceed 90 credit hours for the Undergraduate program and 18 credit hours for the Master of Science in Cyber Security program. Transfer credits may not be used to meet credit requirements for the Graduate Certificates. Transfer/Certifications credits are not considered in the calculation of the student's ECCU cumulative GPA.

Transferability of EC-Council University Credit

Decisions concerning the acceptance of credits or degrees earned at EC-Council University are at the discretion of the receiving institution. Students considering continuing their educations at, or transferring to, another institution must not assume that credits or degrees earned at ECCU will be accepted by the receiving institution. An institution's licenser or accreditation does not guarantee that credits or degrees earned at that institution will be accepted for transfer by any other institution. Students must contact the registrar of the receiving institution to determine what credits or degrees earned that the other institution will accept.

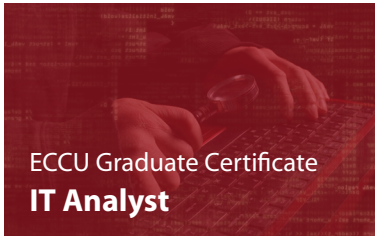
PROGRAMS OF STUDY

Undergraduate Program:

Bachelor of Science in Cyber Security

Graduate Programs:

Master of Science in Cyber Security
Graduate Certificate Program



Bachelor of Science in Cyber Security

Bachelor Program Description

The Bachelor of Science in Cyber Security Program (BSCS) delivers fundamental IT security principles and real-world cyber security applications, tools, and techniques used in today's job work force for careers in Cyber security. It prepares students to obtain knowledge for careers in information technology, and specifically in cyber security. The program features a state of the art virtual labs environment to allow students hands on experience in using the tools of a cyber security professional in a safe, secure sandbox. Covering areas dealing with network management, computer security, incident response, and cyber security threat assessment, the program prepares the student for any entry level position in the cyber security field.

BSCS Program Objectives

Developed from a learning model based on Bloom's Taxonomy of Thinking, the programs educational objectives identify what students should learn, understand, and be able to do as a result of their studies with ECCU. These program objectives are:

1. Application of technical strategies, tools and techniques to provide security for information systems
2. Adherence to a high standard of ethical behavior.
3. Use of research in both established venues and innovative applications to better provide risk assessment, policy updates and security for established enterprise systems
4. Understand the importance of critical thinking to creatively and systematically solve the problems within the parameters of existing information systems
5. Achieve the competency skills needed to fulfill position requirements in the cyber security field

Bachelor's Degree Graduation Requirements

- In addition to the specific degree requirements, each candidate for graduation must meet the following requirements.
- Completion of 60 credit hours of 300/400 level courses in which the candidate earned a cumulative GPA of 2.5 or better
- Completion of 120 + total credit hours including all transfer credit awarded.
- Satisfactory completion of the summative capstone course
- All degree requirements must be completed within four years from the date the student enrolls in the University and begins the program.

Bachelor degree core requirements
All courses are 3 Credit Hours
45 credits required

CIS 300 - *Fundamentals of Information Systems Security ref pg 22 (CSCU).....3 Credits
CIS 301 - Legal Issues in Information Security, pg 22 .....3 Credits
CIS 302 - Managing Risk in Information Systems. pg 23.....3 Credits
CIS 303 - Security Policies and Implementation Issues pg 23 .....3 Credits
CIS 304 - Auditing IT Infrastructures for Compliance pg 23.....3 Credits
CIS 308 - Access Control, Authentication, and Public Key Infrastructure pg 24 .....3 Credits
CIS 401 - Strategies in Windows Platforms and Applications pg 24.....3 Credits
CIS 402 - Security Strategies in Linux Platforms and Applications pg 25.....3 Credits
CIS 403 - Network Security, Firewalls, and VPNs pg 25(CND) .....3 Credits
CIS 404 - *Hacker Techniques, Tools, and Incident Handling pg 26 (CEH).....3 Credits
CIS 405 - Security Strategies in Web Applications and Social Networking pg 26...3 Credits
CIS 406 - *System Forensics, Investigation, and Response pg 27 CHFI .....3 Credits
CIS 407 Cyber-warfare pg 27.....3 Credits
CIS 410 Capstone pg 28.....3Credits

Electives: All courses must be taken unless transfer credit is approved

***Lab Fees**

MTH 350 - Introduction to Statistics pg 29.....3 Credits
BIS 430 - Ethics for the Business Professional pg 30 .....3 Credits
COM 340 - Communications and Technical Writing .....3 Credits

Electives – Must complete two of the three below:

PSY 360 - Introduction to Social Psychology pg 28.....3 Credits
ECN 440 - Principles of Microeconomics pg 30.....3 Credits
MGT 450 - Introduction to Project Management pg 31.....3 Credits

Total credit hours required for the BSS Program.....60 Credits

COURSE DESCRIPTIONS

Undergraduate level Courses

CIS 300 - **Fundamentals of Information Systems Security (3 Credits)** provides a comprehensive overview of the essential concepts readers must know as they pursue careers in cyber security systems. Part one opens with a discussion of the new cyber security risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part Two is adapted for the official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The text closes with a resource for readers who desire additional material on cyber security standards, education, professional certifications, and compliance laws.

Key Features

- Focuses on new risks, threats, and vulnerabilities associated with the transformation to a digital world
- New sections on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development
- Includes changes in laws, security certificates, standards, amendments, and proposed Federal Information Security Amendments Act of 2013.
- Provides new and updated data, statistics, tables, and cases
- Presents a high-level overview of each of the seven domains within the (ISC)2 System Security Certification Practitioner certification

CIS 301 - **Legal Issues in Cyber Security (3 Credits)** addresses the area where law and cyber security concerns intersect. cyber security systems and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous cyber security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers.

Key Features

- Includes discussions of amendments in several relevant federal and state laws and regulations since 2011
- Reviews relevant court decisions that have come to light since the publication of the first edition
- Includes numerous cyber security data breaches highlighting new vulnerabilities

CIS 302 - **Managing Risk in Information Systems (3 Credits)** provides a comprehensive overview of the SSCP® Risk, Response, and Recovery Domain in addition to providing a thorough overview of cyber security risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates handson activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk.

Key Features

- Provides a modern and comprehensive view of cyber security policies and frameworks
- Examines the technical knowledge and software skills required for policy implementation
- Explores the creation of an effective cyber security policy framework
- Discusses the latest governance, regulatory mandates, business drives, and legal considerations.

CIS303 - **Security Policies and Implementation (3 Credits)** Issues offers a comprehensive, end-to-end view of cyber security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. Written by an industry expert, it presents an effective balance between technical knowledge and soft skills, and introduces many different concepts of cyber security in clear simple terms such as governance, regular mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of cyber security policies and frameworks.

Key Features

- Offers a comprehensive, end-to-end view of cyber security policies and framework.
- Addresses the technical knowledge and software skills required for policy implementation.
- Covers governance, regulator mandates, business drivers, and legal considerations.
- Provides an excellent starting point for the creation of an effective IT security policy framework

CIS304 - **Auditing IT Infrastructures for Compliance (3 Credits)** provides a unique, in-depth look at recent U.S. based Information systems and IT infrastructures compliance laws in both the public and private sector. Written by industry experts, this book provides a comprehensive explanation of how to audit IT infrastructures for compliance based on the most recent laws and the need to protect and secure business and consumer privacy data. Using examples and exercises, this Second Edition incorporates numerous hands-on activities to prepare readers to skillfully complete IT compliance auditing.

Key Features

- Includes updates on new pertinent laws and regulations, including FISMA and DoD
- References all new standards such as COBIT, SANS, ISACA, ISO/IEC 27001 and CRMA
- New sections added on the Children's Online Privacy Protection Act (COPPA)
- Service Organization Control (SOC) Reports
- the NIST Cyber Security Framework
- Certification in Risk Assessment (CRMA

CIS308 - **Access Control (3 Credits)** protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the cyber security risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides a student and professional resource that details how to put access control systems to work as well as testing and managing them.

Key Features

- Updated references to Windows 10 and Outlook 2011.
- A new discussion of recent Chinese hacking incidents.
- Examples depicting the risks associated with a missing unencrypted laptop containing private data.
- New sections on the Communications Assistance for Law Enforcement Act (CALEA) and granting Windows folder permissions are added.
- New information on the Identity Theft Enforcement and Restitution Act and the Digital Millennium Copyright Act (DMCA).

CIS 401- **Security Strategies in Windows Platforms and Applications (3 Credits)** focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. The majority of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and stepby-step examples, this must-have resource will ensure readers are educated on the latest Windows security.

Key Features

- New information on Windows 2012 and its four different editions
- New information on malware, ransomware, and spyware
- The latest on Agile Software Development, including its history, purpose, and definition
- Discussion of hacktivists and examples of some of their recent attacks
- New information on Windows 2012 and DAC, Managed Service Accounts, and Expression-based Security Audit Policy
- Discusses new BitLocker features

CIS 402 - **Security Strategies in Linux Platforms and Applications** covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion of the risks, threats, and vulnerabilities associated with Linux as an operating system using current examples and cases. Part 2 discusses how to take advantage of the layers of security available to Linux–user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system.

Key Features

- Focuses on Linux as a server operating system.
- Covers every major aspect of security on a Linux system.
- Uses examples from Red Hat Enterprise Linux and Ubuntu Server Edition, two of the major distributions built for servers.
- Explores open source and proprietary tools when building a layered security strategy for your Linux operating system.
- Offers step-by-step instructions for identifying weaknesses and creating more secure cyber security systems.

CIS 403 - **Network Security, Firewalls, and VPNs (3 credits)** provide a unique, in-depth look at the major business challenges and cyber security threats that are introduced when an organization's network is connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises from the field, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks.

Key Features

- New information on Internet Protocol Version 4 (IPv4) with clarification on the difference between IPv6 and IPv4
- Discusses some of the faults of DNS

- New information on "Mobile IP" and "Bring Your Own Device"
- Discusses the use of a sniffer tool or Wireshark
- Uncovers VPN implementation via cloud application
- Updated statistical information and industry data

CIS 404 - **Hacker Techniques, Tools, and Incident Handling (3 Credits)** begins with an examination of the landscape, key terms, and concepts that a cyber security professional needs to know about hackers and cyber computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by a subject matter expert with numerous real-world examples, the Second Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

Key Features

- Includes a completely new Chapter 13 on social engineering and what it means in the context of cyber security, including a typical attack, identity theft, and best security practices
- Provides new information on cryptography and encryption in network protocols
- Updated references to Windows 8, Server 2008, Server 2012
- Added information on Active Directory and Symantec Security Suite 10
- Includes new material on using social networks, War driving and War flying, detecting rogue access points and Wi-Fi Pineapple
- New section material on cloud computing and cloud security issues.

CIS 405 - **Internet Security: How to Defend Against Attackers on the Web (3 Credits)** provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, the book explores the evolutionary changes that have occurred in data processing and computing, personal and business communications, and social interactions and networking on the Internet. It goes on to review all the cyber security risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet. Using examples and exercises, the Second Edition incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

Key Features

- Securing Mobile Communications
- Addresses the latest Web security issues and solutions from administrator, developer, and user perspectives
- Examines mobile device and connectivity security

CIS 406 - **System Forensics, Investigation, and Response (3 Credits)** begins by examining the fundamentals of cyber security system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. Computer crimes call for forensics specialists, people who know how to find and follow the evidence. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field.

Key Features

- The Second Edition includes all new content. A complete re-write of the first edition
- The latest data and statistics on computer forensics
- Special coverage on:
- Email Forensics
- Windows Forensics
- Mac Forensics
- Linux Forensics
- Mobile Forensics

CIS 407 - **Cyber Warfare (3 Credits)** puts students on the real-world battlefield of cyberspace! Students will learn the history of cyber warfare, techniques used in both offensive and defensive information warfare, and how cyber warfare is shaping military doctrine. Written by subject matter experts, this book combines accessible explanations with realistic experiences and case studies that make cyber war evident and understandable in this evolving cyber security world.

Key Features

- Incorporates hands-on activities, relevant examples, and realistic exercises to prepare readers for their future careers.
- Includes detailed case studies drawn from actual cyberwarfare operations and tactics.
- Provides fresh capabilities information drawn from the Snowden NSA leaks.

CIS 408 - **Wireless and Mobile Device Security (3 Credits)** explores the evolution of wired networks to wireless networking and its impact on the corporate world. The world of wireless and mobile devices is evolving day-to-day, with many individuals relying solely on their wireless devices in the workplace and in the home. The growing use of mobile devices demands that organizations become more educated in securing this growing technology and determining how to best protect their assets. Using case studies and real-world events, it goes on to discuss risk assessments, threats, and vulnerabilities of wireless networks, as well as the security measures that should be put in place to mitigate breaches. The text closes with a look at the policies and procedures in place and a glimpse ahead at the future of wireless and mobile device security.

Key Features

- Incorporates hands-on activities, relevant examples, and realistic exercises to prepare readers for their future careers.
- Includes detailed case studies drawn from real word events.
- Discusses the history and evolution of wireless networks
- Explores the impact of wireless on the corporate world

CIS 410 - **Capstone Course (3 credits)**
This course serves as a comprehensive assessment of knowledge and skills in cyber security systems and cyber security. Activities include research into selected security problems and planning, designing and implementing security solutions for a user organization.

Key Features

- Prepare a Request for Proposal (RFP) content and purpose
- Present a Survey of existing security controls
- Analyze current security gaps and present a formal report
- Create a design of approaches to address security gaps
- Communicating proposed cyber security solutions through an RFP response

PSY 360 - **Social Psychology (3 Credits)**
Why do individuals behave in a certain manner? How do relationships, people, and society influence such behaviors? The purpose of this course is to introduce you to the field of social psychology, but more specifically to help you understand how others influence our behaviors. This course will provide a general overview of human behavior in a social matrix. The course will explore topics and concepts such as: social psychology research, the self, prejudice and discrimination, attraction, relationships, aggression, socialization and conformity.

Key Features

- Apply proper research techniques to produce comprehensive writings by utilizing course texts, readings, discussions, and presentations.
- Discuss and critique topics in weekly group collaboration and activities to develop diverse and critical perspectives.
- Identify and describe the terminology relevant to social psychology.
- Recognize social behavior concepts along with their motivation and influences. Apply these concepts to real-life phenomena.
- Examine the methodology used by social psychologists.
- Analyze and interpret statistical data presented in social psychology research.

MTH350 - **Introduction to Statistics**

Introductory Statistics will familiarize students with a broad base of concepts in probability and statistical methods. Students will learn how to collect, analyze and interpret numerical data and descriptive statistics, create basic probability models, and use statistical inference. This course stresses a wide variety of relevant applications and students will understand how to interpret and critically analyze research data and apply statistical reasoning and interpretation.

Key Features

- Explain the general concepts of statistics.
- Present and describe graphical data.
- Analyze data using regression and correlation.
- Interpret probability distributions for random variables.
- Compute and interpret point and interval estimates.
- Perform hypothesis tests.
- Think critically about information consumed in daily life and use an understanding of statistics to make good decisions based on that information (statistical literacy).

COM 340 **- Communications and Technical Writing (3 Credits)**

This course is designed to prepare you in the basics of cyber security research and writing. You will learn the fundamentals of writing: tips and strategies, critiquing, preparing for a research paper, designing an outline, developing both a thesis statement and a conclusion, and referencing your work. You also will learn how to tell if a website is credible/trustworthy. The information you acquire in this course will help you succeed in your courses to follow, including your final capstone project.

Key Features

- Acquire appropriate communication skills
- Learn to navigate and use available resources
- Determine when a website is credible for use in research and writing
- Learn how to overcome obstacles when writing
- Demonstrate considerate critiquing **check this
- Develop an ability to review and write a comprehensive paper with reference page
- Engage in group discussions (collaboration) and activities to develop critical perspectives, a clear sense of audience- in an effective manner
- Develop accurate and concise writing skills
- Demonstrate the use of correct citation standards

BIS 430 - **Ethics for the Business Professional (3 Credits)**
What is the right thing to do? What is the ETHICAL thing to do? This course will introduce the principles of ethics (moral philosophy) through a variety of topics and dilemmas. We will examine the ideas of goodness, badness, wrongness, and rightness. We will learn about ethical theories of philosophers and apply the knowledge to current events to better understand morality, obligation, human rights, and human nature.

Key Features

- Apply proper research techniques to produce comprehensive writings by utilizing course texts, readings, discussions, and presentations.
- Discuss and critique topics in weekly group collaboration and activities to develop diverse and critical perspectives.
- Identify and describe the terminology relevant to ethics, human nature and morality
- Recognize ethical and moral behavior and its motivation.
- Examine ethical theories and methodologies used to determine goodness and rightness.
- Analyze and interpret statistical data and the review of literature.

ECN 440 - **Principles of Microeconomics (3 Credits)**
Economics is the study of how a society manages its resources. In most societies, resources are allocated through combined choices of their individual members. Economists study how people make decisions, how they work, what they buy, how much they save, and how they invest those savings. Economists also study how people interact with one another. Finally, economists analyze forces and trends that affect the economy as a whole, including the growth of income, the fraction of the population that cannot work, and the rate at which prices are rising or falling. This course covers these concepts and more.

Key Features

- Concepts in trade
- Marketing forces of Supply and demand
- Government policies and their effect
- Taxation
- Competitive Markets and Monopolies
- Cost of Production
- Earnings, Poverty and discrimination
- Theory of Consumer Choice

MGT 450 - **Introduction to Project Management (3 Credits)**
Gaining a strong understanding of IT project management as you learn to apply today's most effective project management tools and techniques are skill sets covered in this class. The course emphasizes the latest developments and skills to help you prepare for the Project Management Professional (PMP) or Certified Associate in Project Management (CAPM) exams. While the PMBOK® Guide is discussed, the course goes well beyond the guide to provide a meaningful context for project management.

Key Features

- Illustrate the factors that influence the success of the project define and explain how to create an cyber security project plan
- Identify the requirements of the IT infrastructure, and compare and contrast the role of IT security project team and Incident Response team
- Examine various project parameters and processes, and recommend how to integrate them into the cyber security project
- Explain the General cyber security project plan and assess the risk factors associated with it
- Evaluate the WBS, explain risk management, summarize the incident response and disaster recovery processes, and formulate risk mitigation strategies
- Design an IT security project plan, organize the processes, predict risks, and illustrate the role of Change Management
- Examine how auditing and documentation processes help in managing the IT security project
- Test the quality of the project, evaluate the factors involved in closing the project and demonstrate how legal standards affect the security strategy

MASTER OF SCIENCE IN CYBER SECURITY

Master of Science in Cyber Security (MSCS) Program Description

The Master of Science in Cyber Security (MSCS) Program prepares information technology professionals for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and cyber security threat assessment, which require students to be creators of knowledge and inventors of cyber security processes, not merely users of information. Additionally, students will receive instruction in leadership and management in preparation for becoming cyber security leaders, managers and directors.

MSCS Program Objectives

Developed from a learning model based on Bloom's Taxonomy of Thinking, the program's educational objectives identify what students should learn, understand, and be able to do as a result of their studies with ECCU. The program objectives are:

1. Application of cyber security technical strategies, tools and techniques to secure data and information for a customer or client.
2. Adherence to a high standard of cyber security ethical behavior.
3. Use of research in both established venues and innovative applications to expand the body of knowledge in cyber security.
4. Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the everchanging environments of cyber security.
5. Mastery of the skills necessary to move into cyber security leadership roles in companies, agencies, divisions, or departments.

Master's Degree Graduation Requirements

In addition to the specific degree requirements, each candidate for graduation must meet the following requirements.

- Completion of thirty-six (36) credits of 500 level courses in which the candidate earned a cumulative GPA of 3.0 or better;
- Satisfactory completion of the summative capstone course;
- All degree requirements must be completed within four years from the date the student enrolls in the University and begins the program.

MSCS Course Requirements (Core and Information Assurance or Management Emphasis)

Core Requirements (21 Credits - required for Graduation)

ECCU 500 - *Fundamentals of Information Systems Security ref pg 37 (CND) ..... 3 Credits
ECCU 501 - *Legal Issues in Information Security, pg 37 (CEH) ..... 3 Credits
ECCU 502 - *Managing Risk in Information Systems. pg 38 (CHFI) ..... 3 Credits
ECCU 503 - *Security Policies and Implementation Issues pg 39 (ESCA) ..... 3 Credits
ECCU 504 - Auditing IT Infrastructures for Compliance pg 39 ..... 3 Credits
ECCU 505 - Access Control, Authentication, and Public Key Infrastructure pg 40 ..... 3 Credits
ECCU 506 - *Conducting Penetration and Security Tests Disaster Recovery pg 40 (LPT) ..... 3 Credits

Choose either 1. Information Assurance or 2. Management as your degree emphasis:

1. Information Assurance Emphasis (select 15 credits from the following courses)

ECCU 507 - Linux Networking and Security pg 41 ..... 3 Credits
ECCU 509 - Securing Wireless Networks pg 41 ..... 3 Credits
ECCU 510 - Secure Programming pg 42 ..... 3 Credits
ECCU 512 - Beyond Business Continuity pg 43 ..... 3 Credits
ECCU 515 - Project Management in IT Security pg 45 ..... 3 Credits
ECCU 516 - The Hacker Mind: Profiling the IT Criminal pg 45 ..... 3 Credits
ECCU 517 - Cyber Law pg 46 ..... 3 Credits
MGMT 502 - Business Essentials pg 47 ..... 3 Credits
Final Course required ECCU 519 CAPSTONE (3 Credit) pg 47 ..... 3 Credits

Total credits hours required fro the MSCS program: 36 Credits

2. Management Emphasis

ECCU 511 Global Business Leadership pg 43 ..... 3 Credits
ECCU 512 Beyond Business Continuity: Managing Organizational Change pg 43 ..... 3 Credits
ECCU 514 Quantum Leadership pg 40 OR MGMT 502 Business Essential pg 47 ..... 3 Credits
Please select 6 credits from the following courses:

ECCU 513 Disaster Recovery pg 44 (EDRP) ..... 3 Credits
ECCU 515 Project Management in IT Security pg 45 ..... 3 Credits
ECCU 516 Th e Hacker Mind: Profiling the IT Criminal pg 45 ..... 3 Credits
ECCU 517 Cyber Law pg 46 ..... 3 Credits

Final Course required ECCU 519 CAPSTONE (3 Credit) pg 47 ..... 3 Credits

Total credits hours required fro the MSCS program: ..... 36 Credits

Graduate Level Courses

ECCU 500 Managing Secure Network Systems (3 credits)
This course focuses on evaluating network and Internet cyber security issues, designing, implementing successful security policies and firewall strategies, exposing system and network vulnerabilities and defending against them. Topics include network protocols, network attacks, intrusion detection systems, packet filtering and proxy servers, Bastion host and honey pots, hardening routers, hardening security, E-Mail security, virtual private networks and creating fault tolerance. CNSS 4011

Key Features

- Describe fundamental networking concepts, analyze networking protocols and implement established standards to design a robust networking infrastructure
- Assess potential vulnerabilities and threats to network infrastructure, predict the implication of network security breaches and analyze the available countermeasures
- Examine different network cyber security mechanisms, analyze available security controls and develop strategies to implement and configure these controls
- Evaluate the role of network security policies, and develop comprehensive policies that help in protecting network infrastructure
- Describe the working of various networking devices, and develop strategies for secure configuration of these devices
- Identify security issues with operating systems and network-based applications, analyze the common vulnerabilities and implement best practices to harden networks
- Analyze cryptography algorithms and encryption techniques, and design implementation strategies for privacy and security of information
- Compare and contrast various network security tools, and make decisions to deploy proper security tools based on evidence, information, and research
- Evaluate physical security mechanisms, examine the issues and recommend the countermeasures to safeguard the network infrastructure
- Examine the impact of an incident in the network and develop policies, processes and guidelines for incident handling and disaster recovery

ECCU 501 Ethical Hacking and Countermeasures 3 credits
This course focuses on how perimeter defenses work, how intruders escalate privileges, and methods of securing systems. Additional topics include intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and virus creation. CNSS 4013A

Key Features

- Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.

- Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing cyber security of various components of cyber security systems.
- Compare and contrast different cyber security hacking techniques and analyze the legal implications of hacking.
- Examine different cyber security vulnerabilities, threats and attacks to information systems and recommend the countermeasures.
- Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information
- Compare and contrast various network security assessment and hacking tools.
- Assess various network security techniques and tools and implement appropriate level of cyber security controls based on evidence, information, and research.

ECCU 502 Investigating Network Intrusions and Computer Forensics (3 credits)

This course focuses on cyber-attack prevention, planning, detection, and incident response with the goals of counteracting cyber-crime, cyber terrorism, and cyber predators, and making them accountable. Additional topics include fundamentals of computer forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity, computer security policies and guidelines, and case studies. CNSS 4012

Key Features

- Describe computer crime and computer investigation process and develop skills associated to the cyber security professional actively helpful in the field of computer forensics and Incident handling.
- Acquire, extract, and analyze all the relevant cyber security digital evidence from computing devices using the most appropriate industry-accepted procedures and techniques to investigate computer crime.
- Consider different perspectives of data acquisition and duplication and develop an organizational strategy on investigating and monitoring the logs that will uphold in the court of law.
- Understand the structure of file systems and hard disk and recover hidden/deleted files or partitions.
- Understand various cybersecurity attacks and Internet crimes and use the set of procedures accepted by court of law to investigate Internet crimes.
- Compare and contrast different forensic tools used in Forensics Investigations.
- Identify the ethical and legal implications used in the gathering, preserving, documenting, and dispatching of forensic evidence that will be upheld in the court of law.

ECCU 503 Security Analysis and Vulnerability Assessment (3 credits)
This course focuses on testing methods and techniques to effectively identify and mitigate risks to the cyber security of a company's infrastructure. Topics include penetration testing methodologies, test planning and scheduling, information gathering, password cracking penetration testing and security analysis, social engineering penetration testing and security analysis, internal and external penetration testing and security analysis, router penetration testing and security analysis, and reporting and documentation. *Prerequisite 501.* CNSS 4014

Key Features

- Monitor, capture and analyze network traffic and identify the possible cyber security breaches
- Identify the various computer security issues and select suitable framework to evaluate security policies, procedures, and controls
- Compare and contrast various network security assessment tools
- Assess various network security techniques and design appropriate protection levels that adhere to network security ethics

ECCU 504 Foundations of Organizational Behavior for the IT Practitioner (3 credits)
This foundation course deals with organizational behavior and allows the technology practitioner to experience the basic facets of organizational theory and defining requisite skills. This course walks the cyber security practitioner through who he/she is as an individual worker and, how he/she fits into an organizational process, defines organizational structure, and articulates elements of effective communication, team building/leading, and project management as seen through the organizational lens. The final component allows the practitioner to work through a case study and design the organizational structure and the behavioral consequences the characters of the study display. From this case study the student will clearly see how the character's behaviors impinge upon the structure in a variety of ways.

Key Features

- Contrast the challenges of global competitiveness with creating and building responsible organizations that take pride in their IT accuracy during sustainable rapid changes.
- Describe the basic organizing concepts of work specialization, span of control, chain of command and authority within IT and IA departments.
- Compare and contrast the three views of ethics in decision-making within your organization.
- Describe the techniques for overcoming communication barriers between IT departments and remaining staff departments.
- Justify which motive there is in managing organization ethics with the IT staff and key players of your organization.
- Internalize and practice the essential skills of leadership in IT units as well as the other departments, which often affect the central mechanism to organization behaviors.

ECCU 505 Introduction to Research and Writing for the IT Practitioner (3 credits)
This foundational core course introduces students to basic English writing skills and research methods, including: APA style writing, citing sources, determining when a website is credible, effective communication, outlines, and collaboration. Students will write/present portions of the above in the course in various formats.

Key Features

- Acquire appropriate communication skills
- Learn to navigate and use available resources
- Determine when a website is credible for use in research and writing
- Learn how to overcome obstacles when writing
- Demonstrate considerate critiquing
- Develop an ability to review and write a comprehensive paper with reference page
- Engage in group discussions (collaboration) and activities to develop critical perspectives, a clear sense of audience- in an effective manner
- Develop critical attitudes toward media and recognize propaganda
- Demonstrate proper citing of sources

ECCU 506 Conducting Penetration and Security Tests (3 credits)
This course focuses on mastery of the international standard for penetration testing. Topics include customers and legal agreements, penetration testing planning and scheduling, information gathering, external and internal network penetration testing, router penetration testing, firewalls penetration testing, intrusion detection system penetration testing, wireless networks penetration testing; password cracking penetration testing, social engineering penetration testing, PDA and cell phone penetration testing, and penetration testing report and documentation writing. *Prerequisite ECCU 503.* CNSS 4015

Key Features

- Examine various penetration testing mechanisms, and choose suitable set of tests that balance cost and benefits.
- Examine the penetration testing techniques that perform the intensive cyber security assessments required to effectively identify and mitigate risks to the security of your infrastructure.
- Demonstrate the compliance of the cyber security system (BS7799, HIPAA etc.) and adopt best practices by conforming to legal and industry regulations.
- Examine various network security devices, test for vulnerabilities and analyze the reports.

- Identify vulnerabilities that could be exploited and predict the effectiveness of additional cyber security measures in protecting information resources from attack.
- Perform internal and external penetration test audits on network infrastructure components and analyze the result.
- Analyze the techniques involved in gathering sensitive information and choose the best way to find the target company's' information.
- Discover any unauthorized access points and check for any services running on the wireless network.
- Examine various password cracking techniques, analyze the sensitive information and predict the implications.
- Examine the post penetration testing actions, analyze the results and present the findings clearly in the final report.

ECCU 507 Linux Networking and Security (3 credits)
This course focuses on configuring a secure Linux network using command line and graphical utilities. Emphasis is placed on file sharing technologies such as the Network File System, NetWare's NCP file sharing, and File Transfer Protocol. Additional topics include making data secure, user security, file security, and network intrusion detection. Students will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur in a work environment. *Prerequisite ECCU 500.*

Key Features

- Effectively use research to understand the fundamentals of Linux platform and analyze the file system.
- Analyze different cyber security vulnerabilities, threats and attacks on Linux systems and networks, and recommend the countermeasures for the same based on relevant research, evidence and references.
- Based on research, examine various security mechanisms available for securing Linux hosts and networks, and then frame policies, guidelines, and best practices for cyber security in the organization.
- Understand the basic Linux networking concepts, examine various networking devices and protocols, and define relevant evidence used to determine strategies for implementing a secure Linux network.
- Compare and contrast various tools to protect, test and monitor the security of Linux systems and implement appropriate level of cyber security controls based on evidence, information, and research.

ECCU 509 Securing Wireless Networks (3 credits)
This course focuses on the various methods of securing wireless networks including authentication, authorization, and encryption. Topics include radio frequency communications, infrared, Bluetooth, low-speed wireless local area networks, high-speed WLANs and WLAN Security, digital cellular telephone, fixed wireless, and wireless communications in business.

Key Features

- Understand the fundamental concepts of wireless network and wireless network security.

- Understand the terminologies, explore the technology trends for next generation wireless networks and examine the functioning of various wireless devices connected to the network.
- Understand how the performance of wireless networks depends on factors such as the protocols used, and assess the role of communication standards in wireless communication system.
- Identify WLAN security issues and design a strategy to manage WLAN Security.
- Examine the various known security risks associated with implementing wireless networks and demonstrate tools to identify the security breaches and analyze wireless security.

ECCU 510 Secure Programming (3 credits)

This course provides the essential and fundamental skills for secure programming. The most prevalent reason behind buggy code and vulnerabilities being exploited by hackers and malicious code is the lack of adoption of secure coding practices. This program will ensure that students are exposed to the inherent security drawbacks in various programming languages or architectures. They will be exposed to exercise secure programming practices to overcome these inherent drawbacks in order to pre-empt bugs from the code.

Key Features

- Understand the importance of secure programming and implement a standard set of secure programming practices, policies, and guidelines to develop robust software applications
- Compare various application development models and methodologies and implement a threat modelling approach to balance between usability and security of applications
- Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information flow in the applications
- Understand the fundamental security concepts used by different programming languages and analyze the usability of different programming constructs in developing secure applications
- Identify the common vulnerabilities, threats and attack vectors in different programming languages, assess the implications and determine the appropriate countermeasures
- Analyze the working of port scanners and hacking tools and write exploits to assess the application security for common attack vectors based on evidence, information, and research
- Understand the security implications of application documentation and error messages and modify default documentation and error message settings so as not to reveal sensitive information
- Compare and contrast different application testing and debugging approaches, develop application testing strategy and explore the ways to avoid classic testing mistakes

- Examine updates, activation, piracy, and other real time application deployment issues and implement controls for secure data communication between various applications
- Compare and contrast different tools that help in developing secure codes and assess the role of these tools in reducing development time and cost thereby adhering to programming ethics

ECCU 511 Global Business Leadership (3 credits)
This course is designed to provide fundamental skills needed to understand global leadership concepts such as developing technological savvy, appreciating diversity, building partnerships, creating shared vision, maintaining a competitive advantage, integrity and leading for change. This is a study of current and historical leadership theories with emphasis on viewing the leadership function in the context of global organizational behavior and organizational designs. *Prerequisite ECCU 505*

Key Features

- Define the 15 dimensions of global leadership
- Explain the value of diversity in organizations
- Demonstrate exceptional leadership
- Evaluate/Analyze a large group of individuals for effectiveness
- Manage large cyber security teams with ease and confidence
- Develop strong partnerships for ultimate performance

ECCU 512 Beyond Business Continuity: Managing Organizational Change (3 credits)
Whether an organization has experienced a disaster, downsizing, a shift in culture or a change in leadership it will experience organizational change. This change demands remembering the past, finding ways to recover from it, engaging the future and energizing change. Leaders in change must have the skills to identify, structure, forecast, envision, design, plan, implement, account for and lead a team through change that has been strategically planned to advance the organization. Such a leader is a change agent and must understand the process, expectations, and nuances of change. *Prerequisite: ECCU 505*

Key Features

- Summarize the two dangers inherent to an information technology-based approach to disaster-recovery
- Examine how a full disaster-recovery plan must consider the contribution of each element of the organization's overall corporate functions
- Determine how individuals and organizations learn from the process
- Understand that success in all fields of Information technology is underpinned by an ability to understand and manage the "human factor.
- Compare the value of an organizational design that advances learning to one that inhibits learning
- Analyze how individuals react to change and how the manager deals with their reaction
- Determine how supervisors serve as Change agents and overcome resistance to change

ECCU 513 Disaster Recovery (3 credits)

This course focuses on cyber security disaster recovery principles including assessment of risks to an enterprise, development of disaster recovery policies and procedures, the roles and relationships of various members of an organization, preparation of a disaster recovery plan, testing and rehearsal of the plan, implementation of the plan, and recovering from a disaster. Additional emphasis is placed on identifying vulnerabilities and taking appropriate countermeasures to prevent information failure risks. CNSS 4016

Key Features

- Understand the various types of disasters and analyze their consequences and effects on organization
- Evaluate the need for cyber security disaster recovery and identify the phases involved in the process of recovery
- Prepare and implement business continuity plan to ensure the protection of organizational assets and business operations
- Assess business risks, frame risk management policies, identify risk management team, and implement solutions to mitigate risks and protect business networks in the event of a disaster
- Analyze the issues related to information system security examine the security mechanism for data backup, role of certification and accreditation authority in securing information systems and identify the technology or services required to recover the data
- Understand laws and acts related to disaster recovery that are applicable in various countries and analyze their impact.
- Assess ethical and legal requirements while undertaking disaster recovery and business continuity services
- Understand various virtualization platforms, assess their roles in disaster recovery, and implement these platforms for optimized resource utilization and availability.

ECCU 514 Quantum Leadership (3 credits)

This course encompasses an extensive research project about cross-cultural differences in leadership conducted by a group of researchers in 62 countries. It lays a foundation of understanding the process of leadership. The study describes the roles, functions and impact of global leadership concepts. The speed at which leadership must adapt to be current is facilitated by numerous team exercises. Research and views into how most cultures respond to this area of management are provided are also compared and discussed. *Prerequisite: ECCU 505*

Key Features

- Develop the role a leader plays in the development and maintenance of the culture.
- Identify the key issues of the GLOBE Research Leadership project.
- Design the three levels of culture along with its individual characteristics.
- Explain the role of individual differences and characteristics in leadership.
- Examine the function of power and its key role in leadership.
- Distinguish between transactional and transformational leadership.
- Explain the leadership practices necessary to implement change.
- Support the idea that leadership development must be considered within the cultural context.

ECCU 515 Project Management in IT Security (3 credits)
This course looks at project management from an cyber security planning perspective - specifically IT Project Management. Students will learn how to use IT framework to develop an effective IT security project plan. This process will help reinforce IT project management skills while providing the student with a road map for implementing IT security in an organization.

Key Features

- Illustrate the factors that influence the success of the project and define and explain how to create a IT security project plan
- Identify the requirements of the IT infrastructure, and compare and contrast the role of IT security project team and Incident Response team
- Examine various project parameters and processes, and recommend how to integrate them into the IT security project
- Explain the General cyber security project plan, and assess the risk factors associated with it
- Evaluate the WBS, explain risk management, summarize the incident response and disaster recovery processes, and formulate risk mitigation strategies
- Design an cyber security project plan, organize the processes, predict risks, and illustrate the role of Change Management
- Examine how auditing and documentation processes help in managing the IT security project
- Test the quality of the project, evaluate the factors involved in closing the project and demonstrate how legal standards affect the security strategy

ECCU 516 The Hacker Mind: Profiling the IT Criminal (3 credits)
Cyber space has increased human communication, connectivity, creativity, capacity and crime by leaps and bounds in the last decade. For all of the positive aspects it offers, it offers as many negative aspects as well. Those negative aspects are explored and developed by everyone from the high school challenge hacker to the international terrorist. Businesses, governmental agencies, militaries, and organizations of every kind are threatened by the IT criminal. This course will survey the full spectrum of psychological attributes which constitute the profile of the IT criminal. *Prerequisite: ECCU 505*

Key Features

- Apply proper research techniques to produce comprehensive writings by utilizing course texts, readings, discussions, and presentations.
- Discuss and critique topics in weekly group collaboration and activities to develop diverse and critical perspectives
- Identify and describe the terminology relevant to cybercrime and criminal profiling
- Recognize criminal behavior, its motivation, and patterns of offenses and apply these concepts to real-life criminals and offenses
- Examine the methodology used to profile a criminal in the cyber world and propose recommendations for future data
- Analyze and interpret statistical data presented in the Hacker Profiling Project (HPP)

ECCU 517 Cyber Law (3 credits)
This course focuses on the legal issues driven by on-line cyber security criminal conduct electronic evidence of a crime, and the legal ramifications of neglecting trademarks, copyrights, patents, and digital rights. Topics include the following: laws, regulations, international standards, privacy laws governing law enforcement investigations in cyberspace implications of cyber crimes upon the traditional notions of sovereignty and current events that affect cyber laws. *Prerequisite ECCU 505*

Key Features

- Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet cyber security
- Discuss different types of cyber crimes and analyze legal frameworks of different countries to deal with these cyber crimes
- Describe the importance of jurisdictional boundaries and identify the measures to overcome cross jurisdictional cyber crimes
- Describe the importance of ethics in legal profession and determine the appropriate ethical and legal behavior according to legal frameworks
- Identify intellectual property right issues in the cyberspace and design strategies to protect your intellectual property
- Assess the legal issues with online trading and analyze applicable e-contracting and taxation regulations
- Frame cyber security policy to comply with laws governing privacy and develop the policies to ensure secure communication
- Describe the importance of digital evidence in prosecution and analyze laws of different countries that govern Standard Operating Procedures (SOP) for handling evidence

ECCU 518 Special Topics (Introduction to Cloud Computing) (3 credits)
Special topics courses will be offered from time to time to pilot a course or to respond to a particular trend in information assurance. These courses will be considered as electives. *Prerequisites ECCU 500 and 505*

Key Features

- The ability to apply knowledge of cloud computing and be able to articulate a migration strategy from legacy open access technologies to cloud technology
- An ability to analyze a problem, and identify and define the cloud computing requirements appropriate to its solution
- Students will know the advantages of applying cloud technology to computing applications, communications and information storage.
- An ability to communicate effectively with a range of audiences
- An ability to analyze the local and global impact of computing on individuals, organizations and society
- An ability to use current information security techniques, skills and tools necessary for cloud computing practice

ECCU 519 Capstone (3 credits)

The Capstone is the summative experience designed to allow students to demonstrate all program objectives and draw on the knowledge and skills learned throughout the entire program. Students can enroll in the Capstone after of successful completion of all core degree requirements but must be within 6 credit hours of graduation Students must attainment of a 3.0 cumulative grade point average and have the registrar approval to register in this class.

Key Features

- Perform assessment of the cyber security needs, analyze the internal and external cyber security threats, and determine and implement the methodologies to secure the cyber security systems of an organization
- Perform an cyber security audit of a complete information system
- Identify a cyber security attack, collect necessary evidence in a forensically sound manner and trace the perpetrator of crime
- Implement the best and most appropriate strategy for re-meditating the situation
- In an effective manner, communicate to the staff or business partners (all constituents and stakeholders) the occurrence, ramifications, etc., of that cyber security attack.
- Create a "protective solution" including auditing and penetration testing of IS to help protect the business or organization from experiencing a similar situation
- Effectively manage all pertinent personnel that is impacted by the cyber attack by designing and implementing standard cyber security policies, procedures and trainings
- Identify the common thread to the organizational impact as well as the security impact of successive network innovations.
- Define a set of useful ideas or "laws of identity" that an IS technician can use to reduce insider threat.

MGMT 502: Business Essentials (3 credits)

This course will lay a broad foundation of understanding the processes of business principles, both globally and for a varied population of students, which comprise those who work in industries of all kinds including the Information Technology and Cyber security fields. It covers the latest changes in Information Technology for Business, also including computer-aided manufacturing (CAM), applications software, and recent ethical issues arising from IT. Real-life business examples are added throughout the course that reinforces the business principles.

Key Features

- Explain the importance of the economic environment to business and analyze the factors used to evaluate the performance of an economic environment.
- Describe each of the common legal and political issues among nations that affects international business: quotas, tariffs, subsidies, and business practice laws, etc.
- Demonstrate how companies with different business strategies are best served by having different operations capabilities.
- Evaluate leadership decision making by discussing rational and behavioral perspectives.
- Identify the 5 "forces" that constitute the external marketing environment and influence its organizational goals.
- Aside from the impact of Information Technology has on the business world, identify the threats and risks IT cyber security poses for businesses
- Discuss some of the institutions and activities in international banking structures and global finance.

GRADUATE CERTIFICATE PROGRAM

The EC-Council Graduate Certificate Program provides the opportunity for students to start advanced education and complete it in two or three terms instead of the two or three years required by the full master's degree. These course focused certificates allow students to sharpen skills, deepen knowledge, and develop a specialty. The certificates can be added to a student's professional portfolio and used for career change or advancement. Graduate certificate courses are the same courses required for the Master of Security Science, simply bundled in highly focused groupings.

There are five EC-Council University Graduate Certificates - Cyber Security Professional, IT Analyst, Digital Forensics, Disaster Recovery, and Executive Leadership in Cyber security. Please see the specific course requirements for each certificate listed in this catalog.

Students desiring to pursue a graduate certificate must meet the same admission requirements as those seeking the Master of Science in Cyber Security and are subject to all University policies and procedures. Course work completed as a part of a graduate certificate can be applied to the MSCS degree within five years of completion.

ECCU Graduate Certificates

* Must meet prerequisites in course descriptions

I. ECCU Graduate Certificate – Information Security Professional **9 Credits**

Required Courses:	ECCU 500 Managing Secure Network Systems	3 Credits
	ECCU 501 Ethical Hacking and Countermeasures	3 Credits
	ECCU 505 Research and Writing for the IT Practitioner	3 Credits

ECCU Graduate Certificate – Information Security Professional is designed to develop the skill set of an entry level Cyber Security Professional, as well as basic system security testing and hardening of a target system. This certificate encompasses for the appropriate education and training for an employee in such a position.

II. ECCU Graduate Certificate – IT Analyst **9 Credits**

Required Courses:	ECCU 504 Foundations of Organizational Behavior for the IT Practitioner	3 Credits
	ECCU 506 Conducting Penetration and Security Tests	3 Credits
	ECCU 513 Disaster Recovery	3 Credits

ECCU Graduate Certificate – IT Analyst is designed to prepare an Cyber Security Professional specializing in Risk analysis and certification of information systems to meet a designated skill set of security standards. A holder of this graduate certificate would be qualified to perform risk assessment and analysis, business impact analysis and participate in a business continuity planning team. Holders would also be qualified to conduct certification and accreditation tasks as well as create and enforce security policies relating to that task.

III. ECCU Graduate Certificate – Digital Forensics* **9 Credits**

Required Courses:	ECCU 502 Investigating Network Intrusions and Computer Forensics	3 Credits
	ECCU 515 Project Management in IT Security	3 Credits
	ECCU 516 The Hacker Mind: Profiling the IT Criminal	3 Credits

ECCU Graduate Certificate – Digital Forensics is designed to demonstrate the required skill set for a Computer Forensic Investigator. Someone with the knowledge and training provided by the courses in this graduate certificate would be qualified for a Digital Forensic Investigator with the government at any level, as well as for a private industry both on, or leading an incident response team.

IV. ECCU Graduate Certificate – Disaster Recovery **9 Credits**

Required Courses:	ECCU 503 Security Analysis & Vulnerability Assessment - CNSS 4014	3 Credits
	ECCU 512 Beyond Business Continuity	3 credits
	ECCU 513 Disaster Recovery - CNSS 4016	3 Credits

ECCU Graduate Certificate – Disaster Recovery is designed to demonstrate a skill set level for a leader in Disaster recovery planning and performance. A holder of this graduate certificate would be qualified to lead a Business Continuity and/ or Disaster Recovery team.

V. ECCU Graduate Certificate – Executive Leadership in Information Assurance

Prerequisite: ECCU Graduate Certificate - Information Security Professional 9 Credits

Required Courses:	ECCU 511 Global Business Leadership	3 Credits
	ECCU 514 Quantum Leadership	3 Credits
	AND	
	ECCU 512 Beyond Business Continuity	3 Credits
	OR	
	ECCU 515 Project Management	3 Credits

Prerequisite: Must hold one of the following: Digital Forensics, IT Analyst, Information Security Professional or Disaster Recovery .

ECCU Graduate Certificate – Executive Leadership in Information Assurance is designed train Chief Information Security Officers the skill set required to lead an efficient and productive team environment. Holders of this graduate certificate could be candidates for C-Level positions with private industry or the equivalent of a government level position.

Testing for EC-Council Certifications

Many classes in the master and bachelor program parallel knowledge requirements for EC-Council certifications. Once a student has completed the corresponding university class then he or she is eligible to test for the certification. Students must pass the certification test to achieve the certification. Receiving a passing grade in the University class is NOT a guarantee of passing the certification exam. While ECCU classes waive the education requirement students are still required to purchase the exam voucher from EC-Council to test for the certification. ECCU has negotiated a student rate for the exam vouchers contact registrar@eccu.edu for more information.

CERTIFICATION	MASTER CLASS	BACHELOR CLASS
CND	ECCU 500	CIS 403
CEH	ECCU 501	CIS 404
CHFI	ECCU 502	CIS 406
ECSA	ECCU 506	
EDRP	ECCU 513	
CSCU		CIS 300

STUDENT SERVICES

Student Services Portal

ECCU has an online portal called Populi, for students. Students can log in to register for classes, view their unofficial transcript, run a degree audit and pay their tuition.

Registering for Courses

Initial registration for each student is included in the Student Enrollment Agreement. After completion of the first term, students may register themselves for subsequent terms. The dates of open registration are published in the academic calendar and registration is completed in Populi. It is recommended that students read the course descriptions in this catalog to ensure that they meet the prerequisites of the next course and carefully plan their schedule. Upon registration, students will be assigned a MyECCU log-in and password. All payments are due by the deadline published in the academic calendar.

Mode and Duration of Study

All courses are offered in twelve-week terms using an online format via the myECCU portal. To be considered a full-time student, a graduate student must take two courses in each term and undergraduate students must take 3 courses per term. Students taking fewer courses a term will be considered part-time. The Master's and Bachelor's programs are designed to be completed in a maximum of four years.

Course Delivery

All classes are delivered online and are asynchronous. Course materials may include discussions, readings, videos, case studies, virtual labs, and games. EC-Council University uses a variety of educational methods to maximize student-learning outcomes. The courses are built around the central components of the instructional processes: presentation of content; interaction with faculty, peers, and resources; practical application; and assessment. Each EC-Council University course uses technologies in various ways to address some or all of these components.

Students are provided a variety of materials for each course, including a detailed syllabus, the list of textbooks, labs and reference materials, and information on how to communicate with the faculty member assigned for the course. The faculty member provides guidance, answers questions, leads online discussions, and evaluates the student's work.

Contact between the student and the faculty member is achieved through one or a combination of the following methods: website, email, EC-Council University's web portal, telephone, voicemail, and/or video-conferencing.

Credits

All credits awarded by EC-Council University are semester hour credits and equate with the formula of 45 clock hours of student work per credit.

Grades

Grades and credits awarded become official once they are recorded on the student's permanent record in the University's administrative office. At the end of each academic period students can check their grades and credits earned on our student information system, Populi. Credits are awarded only upon successful completion of course requirements

Textbooks

Applicable textbooks are used for each course. Required texts are indicated in the course outline and in the course syllabus by title, author, publisher, and ISBN. Some texts are provided to the student in a digital format however, some will have to be purchased separately by the student.

ACADEMIC POLICIES AND GUIDELINES

Academic Load:

In the MSCS program students usually take 3-6 credits per term and 6-12 credits per term in the BSCS program. It is expected that a student will spend about 45 hours of time per credit in class preparation and assignments making the expected time spent by the student per 3 credit course 135 hours per 12-week term or about 13.5 hours per week per class. The maximum number of credit hours a student can take per term in the MSCS program is 9 and in the BSCS program the maximum is 15.

Minimum Academic Achievement:

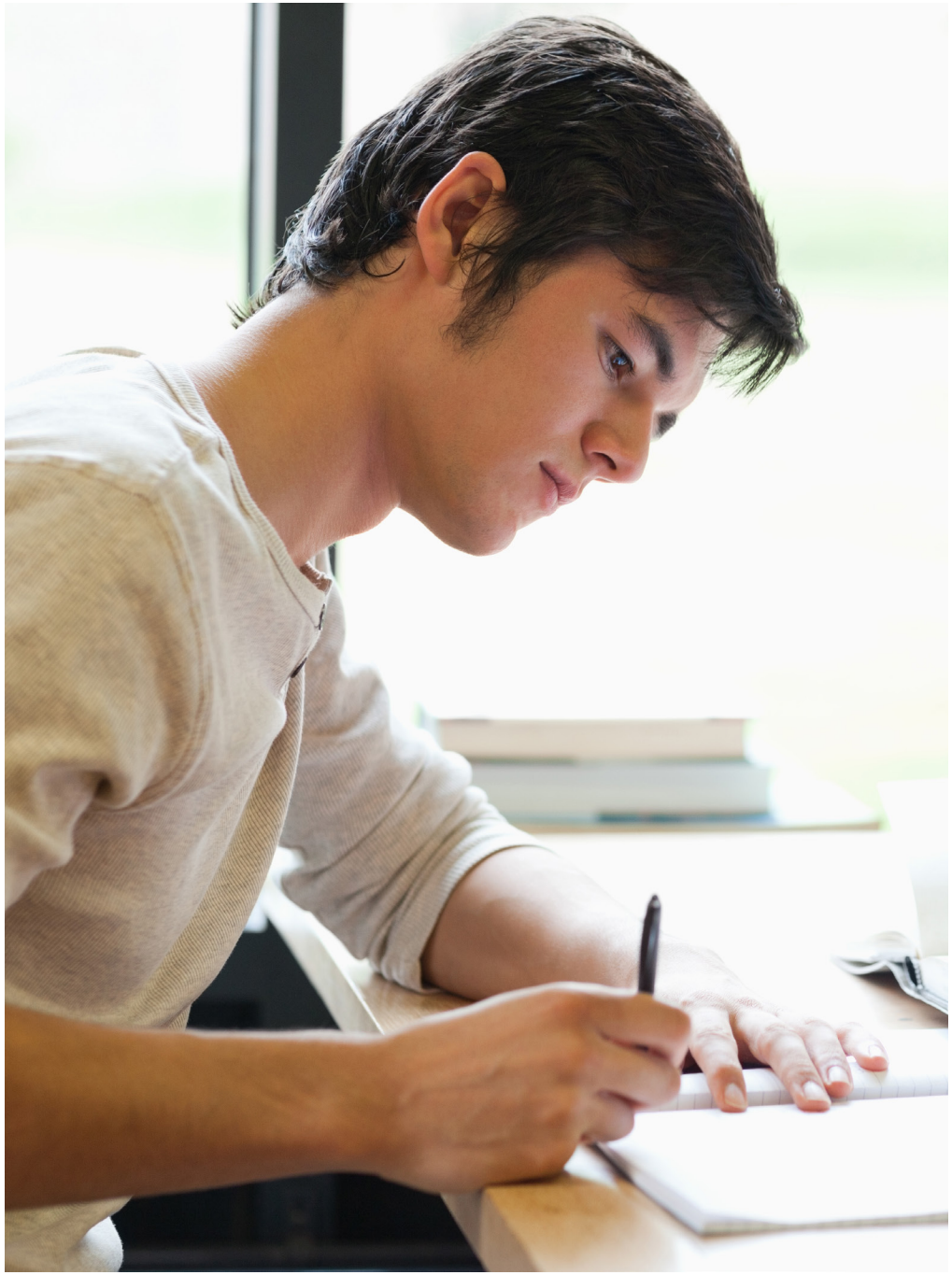
Master's degree candidates must maintain a cumulative GPA of 3.0 or higher. Bachelor degree candidates must maintain a cumulative GPA of 2.5 or Higher. Failure to maintain this GPA will result in being placed on academic probation or suspension.

Maximum Program Length:

A student must complete the entire program within one-and-one-half times the program length or 4 years for both the Master's and Bachelor's degrees.

Attendance and Participation:

Students are expected to participate in all class sessions and assigned activities. Extenuating circumstances which are beyond the control of the student may occur, however, if a student will miss assignments or discussions he or she must contact the instructor in advance. At the faculty member's discretion, the student may be required to make up the work to achieve the allotted points. In extreme cases due consideration will be given.



Missed or Late Assignments:

Missed or late assignments will only be accepted with prior approval from the instructor. Acceptance of missed or late assignments is solely at the discretion of the faculty member, within their established guidelines.

Leaves of Absence:

A Leave of absence (LOA) is an interruption in a student's pursuit of degree at EC-Council University. A LOA could be a minimum of one term, or at most, 5 consecutive terms. LOA's will not exceed 2 granted requests.

There are many reasons that could hinder students' education; health, work, family problems, personal difficulties, natural disasters and civil unrest. EC-Council University recognizes the trials and tribulations that our diverse student population may encounter, therefore we have developed a policy that allows students to take a leave of absence (LOA) from their studies and return to pursue their education without penalty. It is the students' responsibility to notify the ECCU administration when requesting an LOA. Scholarship students should consult with the Registrar prior to requesting an LOA, as it may result in loss of scholarships and affect their rate of tuition. Documentation may be requested by ECCU administration demonstrating the extenuating circumstances.

Students who are absent from the program for one calendar year without requesting a LOA will be considered inactive students. Upon return to the University, they will be required to update their student enrollment agreement and will continue their program under the most current catalog which includes tuition/fee changes and program degree requirements.

Satisfactory Academic Progress

A student must continuously maintain satisfactory academic progress (SAP) toward completion of their degree program, regardless of their course load. SAP is defined as a 3.0 cumulative GPA for graduate students and a 2.5 cumulative GPA for undergraduate students. A student must satisfy the criteria listed below to maintain continuous SAP. Any student who fails to maintain SAP will be notified by the Manager of Enrollment and Student Services and be placed on Academic Probation (AP).

Criteria for maintaining continual SAP:

1. The students Overall Cumulative Grade Point Average (OCGPA) is at least 3.0 on a 4.0 grading scale in the graduate program and 2.5 on a 4.o grading scale for the undergraduate program.
2. The student has successfully completed (received A's, B's, C's, or D's*) fifty percent (50%) of all courses attempted in the program after the first two grading periods (Percentage of Credit Completion-PCC).

*A letter grade of D is not acceptable for a Master's level program and will be required to be retaken.

Academic Probation:

EC-Council University makes a discerned effort to monitor student progress on a continual basis. A major part of this monitoring process is to review student's cumulative GPA (CGPA) every term. Every student admitted to EC-Council University is expected to maintain continual Satisfactory Academic Progress (SAP) every term.
Failure to maintain SAP in any given term will result in the student being placed on academic probation for the next term. Student who do not meet SAP will be referred to the advisor. The advisor will work closely with the student to provide techniques and tools to assist the student to improve their GPA.

Students may be able to improve their CGPA to the required 3.0 the first term that they are on AP and achieve SAP. Other students who have made improvements, but have not raised their CGPA to the required 3.0 will remain on interim academic probation for each subsequent term until achieving the CGPA required 3.0 to register for the Capstone course and graduate. In order to remain eligible for interim academic probation (IAP) the student is required to continually make CGPA improvements each term. Therefore, students are required to earn A's or B's each successive term while on IAP.

If a student fails to make CGPA improvements for two successive probationary grading periods, he/she will be required to complete academic remediation module. The student will have their enrollment suspended while they complete the academic remediation module. Students who successfully complete the academic remediation module may return to classes. If the student earns a B or better in the returning term they may continue on interim academic probation. If they earn a C or lower they will be terminated from the program. Student who do not complete the academic remediation module will be terminated from the program. Students are only eligible for the remediation module one time. If after completing the remediation module and taking a successful term, the student's GPA does not improve each term the student will be terminated from the program.

Students terminated from the program are terminated without refund unless the following occurs:

1. The student appeals the school's determination in writing to the Dean.
2. The Student Academic Appeals Board (consisting of Dean, Registrar, and Advisor) consider a special circumstance and grants the student's appeal.

Cumulative Grade Point Average (CGPA)

The calculation of the students Cumulative Grade Point Average or CGPA in their program will be the total number of credits per course (3) multiplied by the grade points earned (A=4, B=3, C=2, D=1, F=0) divided by the total number of credits earned. Transfer credits are not used to determine CGPA.

Percentage of Credit Completion

Percentage of Credit Completion (PCC) shall be calculated by dividing the total number of credit hours for which a student receives a grade of "A", "B", "C", "D" by the total number of credit hours the student has attempted in their program of study.

Maximum Time of Completion

The student's maximum time of completion for their program of study shall be 150% of the attempted credit hours designated in the program outline rounded down to the nearest whole credit hour. The MSCS Program consists of 36 credits, so the students' maximum time of completion shall be 54 attempted credit hours (36 X 150%).

A student not making SAP will be terminated from their program if the school determines that the student is unable to graduate from their program without exceeding their maximum time of completion.

Academic Suspension:

A student who fails to achieve overall satisfactory academic progress (3.0 cumulative GPA) for the program at the end of two successive probationary grading periods will have their enrollment suspended while they complete the academic remediation module. Students who successfully complete the academic remediation module may return to classes. If the student earns a B or better in the returning term they may continue, if they earn a C or lower they will be terminated from the program. Student who do not complete the academic remediation module will be terminated from the program.

Academic Dismissal/Termination:

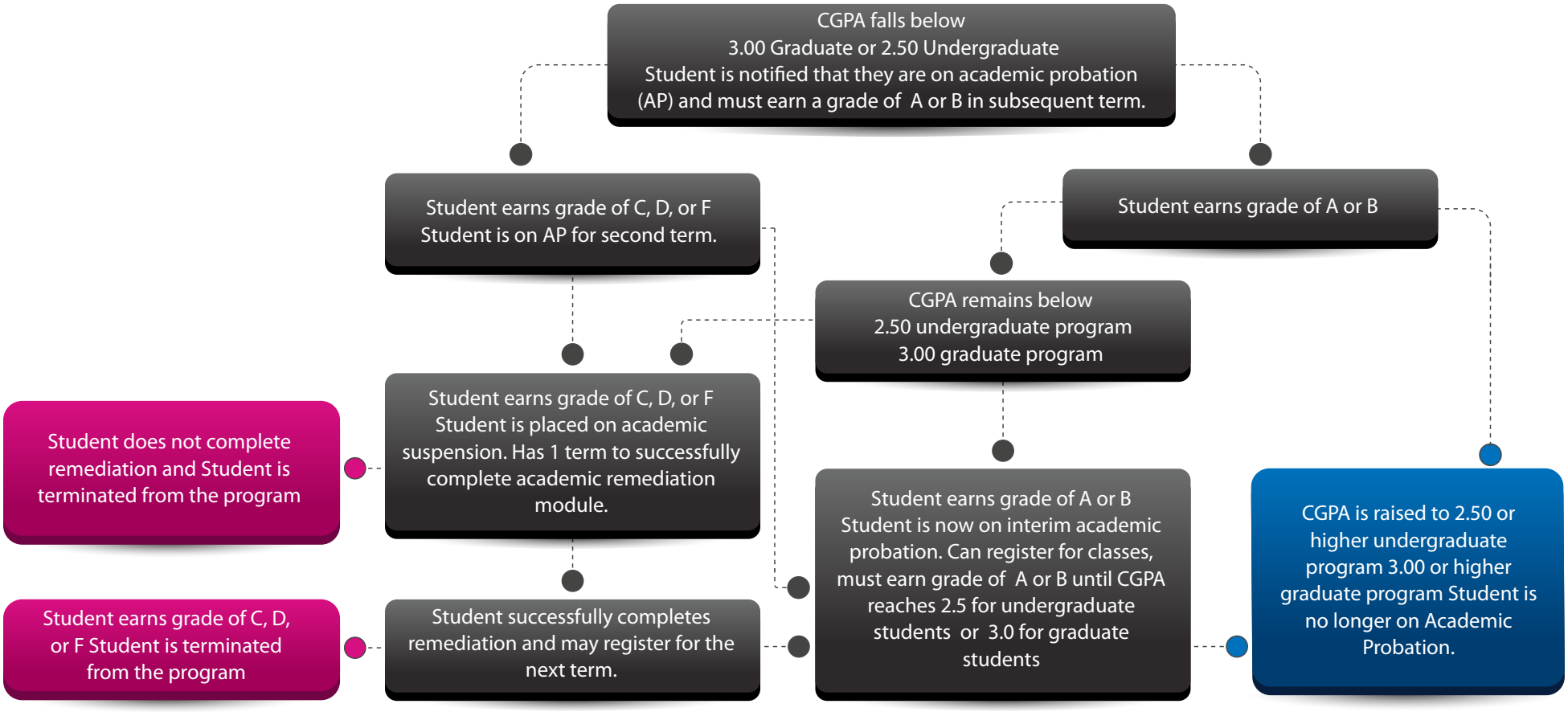
A student that does not maintain satisfactory academic progress (3.0 cumulative GPA) during or by the end of their final probationary period, the student will be terminated without a refund.

Appeal of Probation and/or Dismissal:

Students who have been dismissed from the University due to a failure to keep current with financial obligations to the University must pay any outstanding balance due prior to appealing a probationary or dismissal decision.

Students have the right to appeal any and all academic probation or dismissal decisions by writing to the Dean. The appeal must be in writing and postmarked or emailed no later than 30 days after the student has received notification of the academic probation or dismissal. After receiving the student's appeal request, the Student Academic Appeals Board (consisting of Dean, Registrar, and Advisor) will review the academic probation or dismissal. Within 15 days of receiving the student's appeal, the Dean shall render a final decision and notify the student.

Progression of Academic Probation



ACADEMIC HONESTY POLICY

ECCU Course Policies on Cheating and Plagiarism

As a model of the highest ethical standards and as an institution of higher-learning, EC-Council University expects its students to conduct themselves with an unquestionable level of honesty and integrity. EC-Council University will not tolerate academic cheating or plagiarism in any form. Learning to think and work independently is not only a part of the educational process, it is the educational process. Cheating or plagiarism in any form is considered a serious violation of university policy, of which each student agreed to when accepted into the program. Student academic behaviors that violate the university policy will result in disciplinary action; without exception. University policy can be summarized simply: As a student, you are responsible for your own work and you are responsible for your own actions. Some examples of cheating and plagiarism include but are not limited to:

Cheating	Use of material, information, or study aids not permitted by the faculty
Plagiarism	Use of another's words or ideas without acknowledging the source of the information
Falsification or fabrication	Changing or altering data, quotes, citations, grades or academic records
Unauthorized collaboration	Intentional sharing of information when such collaboration is not approved by the faculty

EC-Council University will take action in all cases of academic dishonesty. The first instance will result in a failing grade for the assignment, the second instance with a failing grade in the class, and the third instance with dismissal from the university. Record of all instances of academic dishonesty and the action taken will be kept in the individual student file and in the Dean's file of all instances of academic dishonesty for the institution.

Steps to be taken in the instance of academic dishonesty are:

1. The faculty/staff will inform the student of the allegation and provide evidence, offering the student the opportunity to respond and/or rectify the issue depending on the nature of the dishonesty and the particular assignment.
2. Once the student has had a chance to respond, the faculty/staff will determine if academic dishonesty has occurred. If the faculty/staff concludes that academic dishonesty has occurred and has proof, they will report the student's name, the class and assignment, the nature of the academic dishonesty and the proof to the Dean. The type of disciplinary action to be taken will be determined by the student's record of instances identified above and will be applied by the faculty and/or the Dean.

Citing Sources

In academic communities, the ethics of research demand that writers be credited for their work and their writing. Not to do so is to plagiarize--to intentionally or unintentionally appropriate the ideas, language, or work of another without sufficient acknowledgement that such material is not one's own. Whenever a student quotes, paraphrases, summarizes, or otherwise refers to the work of another, the student must cite his or her source either by way of parenthetical citation or footnote. Unfortunately, this is the most common form of academic dishonesty, but regardless it will be responded to with failing grades or dismissal.

Original content

Students are expected to create their discussion topics, assignments and essays using the majority of their own personal thoughts and ideas. All works must contain a minimum of 75% original work. Any work submitted that contains more than 25% unoriginal work regardless of whether the sources are cited properly may be considered a violation of the academic honesty policy, depending on the nature of the assignment, and consent of the assigned instructor.

Timeline

Discovery of violation of the Academic honesty policy can occur at any time. Issuance of a grade, or even degree, can be changed if it is discovered that an academic honesty violation occurred. The bottom line is this it's just not worth it.

Student Identity Verification

- EC-Council University takes measures to verify the identity of the students who are applying to the university, completing courses, and taking proctored exams.
- Students access their courses and reference materials through our secure online learning management system, where they are required to enter in their username and password. Each student is responsible for the safeguard of their individual credentials.
- EC-Council University implements student identity verification in several ways to ensure proper ID.

    1. A Valid Government issued ID is required with admissions application.
    2. Login credentials are required for the online LMS portal.
    3. Proctored exams require a valid photo ID to be presented at time of exam as well as a screen shot of ID.

Remote Proctor NOW Exams

- EC-Council University utilizes Remote Proctor NOW (RPN) exam proctoring services for all courses which require a proctored exam. These exams are presented throughout the program at a minimal cost to the student of $15 USD each.
- This secure cloud-based proctoring services allows students to take secure exams at their convenience while maintaining university integrity.
- The exam can be accessed through www.myrpintall.com. More instructions and training videos for utilizing RPN can be viewed. In the New Student Orientation a PC or Mac, webcam (external or built in), and an internet connection are required.

Grading System

The grading system used at EC-Council University is the A-F system (see definitions below). Unless otherwise stated, the University awards letter grades in recognition of academic performance in each course. Grade points are used to calculate grade point average (GPA).

I Incomplete Under some circumstances (i.e. other than lack of effort and study), if all assignments in a course are not completed before its conclusion, the student may request an Incomplete for the course. If the instructor agrees, an "I" will be placed on the student's transcript. The student will have 180 additional days from the end of the term to complete the course and replace the "I" with the assigned letter grade. If, at the end of the normal extension, the student has been unable to complete the course due to extenuating circumstances, s/he may appeal to the Provost for one additional 90-day extension, providing justification as to why they were unable to complete the course. The granting of the Incomplete is at the discretion of the instructor. If the work is not completed before the incomplete expires, the "I" will automatically revert the current earned grade in the course. The student has the right to appeal the instructor's decision to the Provost.

IP In Progress applies to currently enrolled courses.

R Retaken course. An "R" grade is indicated on the transcript when the course grade has been superseded by a later grade. Only the later grade will be used in computing the GPA.

W A student may withdraw from a course by notifying the Registrar in a documented manner (mail, e-mail or Fax). If the withdrawal occurs during an active course, the student will receive a refund as per the refund schedule in the refund policy. A "W" will appear on the student's transcript and the credits for the course will be added to the cumulative credits attempted. Refer to the published academic calendar- dates and deadlines section for dates when withdrawal is allowed.

AW Faculty members or ECCU staff may initiate an Administrative Withdrawal (AW) of a student from a course based on lack of attendance or participation, or lack of connectivity. Please see the description of these items below. Depending on when the AW occurs, the student may be eligible for a refund according to the refund schedule in the refund policy. AW will appear on the student's transcript and the credits for the course will be added to the credits attempted. If the student is administratively withdrawn from the class because of plagiarism, disciplinary action will occur resulting in the student receiving not an AW but an F on their transcript and the protocol described in the Academic Honesty Policy will be employed.

LETTER GRADE	RANGE OF POINTS	GRADE POINTS
A	93.00-100.00	4
A-	90.00-92.00	3.76
B+	90.00-92.00	3.33
B	83.00-86.00	3
B-	80.00-82.00	2.67
C+	77.00-79.00	2.33
C	73.00-76.00	2
C-	70.00-72.00	1.67
D+	66.00-69.00	1.33
D	60.00-65.00	1
F	0.00-59.00	0

**A letter grade of D is not acceptable for a Master's level program.*

Although students can be dropped for lack of attendance or non-participation, the student should never assume that s/he will be automatically withdrawn for any reason.

Lack of Attendance/Participation: During the first two weeks of class, students who fail to attend class meetings or class related activities or fail to participate without contacting the faculty member and making special arrangements will be administratively withdrawn from class. The faculty member is under no obligation to allow students to make up work they have missed because they failed to attend or participate. *Students should never assume that they will be automatically withdrawn by staff for lack of attendance.*

Lack of Connectivity: Students having connectivity problems/issues may be administratively withdrawn. It is the student's responsibility to ensure the equipment needed to complete the requirements of the course is connected, current, and functional for class purposes. Faculty are not responsible for the student's lack of connectivity and are not obligated to allow students to make up work because the student could not connect. Students should never assume that they will be automatically withdrawn by staff for lack of connectivity.

GPA Calculation

Grade point average (GPA) can be calculated by dividing the number of hours in all classes attempted, in which a grade of A, B, C, D or F have been received, into the number of grade points earned in those hours. For example:

The student has completed five classes with the following grades:

ECCU 500 B = 3 grade points x 3 credit hours = 9
ECCU 502 C = 2 grade points x 3 credit hours = 6
ECCU 503 A = 4 grade points x 3 credit hours = 12
ECCU 504 B = 3 grade points x 3 credit hours = 9
ECCU 505 A = 4 grade points x 3 credit hours = 12

Total number of grade points 48
grade points divided by 15 (Total # of hours) = 3.2 GPA

Credits

All credits awarded by EC-Council University are semester hour credits. Credits are awarded only upon successful completion of course or project requirements.

Academic Recognition

Students will graduate with honors if they have a cumulative GPA of:

- Cum Laude - for grade point averages of 3.75 through 3.84
- Magna Cum Laude - for grade point averages of 3.85 through 3.94
- Summa Cum Laude - for grade point averages of 3.95 and above

Grade Appeal

A student may appeal a course grade issued by a faculty member. The appeal must be made to the faculty member from whom the grade was received in writing and must be postmarked or emailed no later than 30 days after the student received notification of the grade. Should the appeal be denied, or if the faculty member does not respond within 15 days after sending the appeal, the student may appeal directly to the Dean within an additional 15-day period. The Dean will render a final decision on the grade within 15 days after receiving the student's appeal.

Withdrawal from Program or Course

The student has the right to withdraw from a course or program by notifying EC-Council University in any manner at:

EC-Council University
101 C Sun Ave NE, Albuquerque, New Mexico 87109
1-505-922-2889
registrar@eccu.edu

The date by which the notification is postmarked, phoned, or emailed is the effective date of the withdrawal. Any tuition or fees owed to the student will be refunded within 30 days of the receipt of the withdrawal notice.

All fees owed to the University are due immediately upon withdrawal. Accounts that have an outstanding balance may be sent to a 3rd party collection service.

RIGHTS AND RESPONSIBILITIES

Student Conduct

Students are expected to be familiar with all published policies and procedures of EC-Council University and will be held responsible for compliance with these policies. The following is a code of conduct that has been written by the Distance Education and Training Council.

A Code of Conduct for the Distance Education Student

I recognize that in the pursuit of my educational goals and aspirations I have certain responsibilities toward my fellow distance learners, my institution, and myself. To fulfill these responsibilities, I pledge adherence to this Code of Conduct.

I will observe fully the standards, rules, policies, and guidelines established by my institution, the state education agency, and other appropriate organizations serving an oversight role for my institution.

I will adhere to high ethical standards in the pursuit of my education, and to the best of my ability will:

1. Conduct myself with professionalism, courtesy and respect for others in all of my dealings with the institution staff, faculty and other students.
2. Present my qualifications and background truthfully and accurately for admission to the institution.
3. Observe the institutional policies and rules on submitting work, taking examinations, participating in online discussions and conducting research.
4. Never turn in work that is not my own or present another person's ideas or scholarship as my own.
5. Never ask for, receive, or give unauthorized help on graded assignments, quizzes, and examinations.
6. Never use outside books or papers that are unauthorized by my instructor's assignments or examinations.
7. Never divulge the content of or answers to quizzes or examinations to fellow students.
8. Never improperly use, destroy, forge, or alter my institution's documents, transcripts, or other records.
9. Never divulge my online username or password.
10. Always observe the recommended study schedule for my program of studies.
11. Always report any violations of this Code of Conduct to the appropriate institution official and report any evidence of cheating, plagiarism or improper conduct on the part of any student of the institution when I have direct knowledge of these activities.

Student Responsibilities

Students must comply with the obligations outlined in the Student Enrollment Agreement and in accordance with any reasonable instructions issued from time to time by or on behalf of the University, listed below, but not limited to:

- Attend assigned enrolled classes
- Submit required course work and other assignments required for the program prior to the prescribed deadlines
- Behave appropriately within the University environment
- Be adequately prepared for any activity required as part of the program outside the University, at all times conducting oneself in a proper manner
- Comply with any professional standards applicable to the program
- Abide by any special conditions relating to the program set out in the catalog or student enrollment agreement, unless otherwise notified by the University
- Provide the registrar with an emergency contact name and details which the University may use at its discretion
- Notify the registrar of any changes to the information which has been submitted on the application or Student Enrollment Agreement; for example, change of address

Faculty Responsibilities

The University faculty members will take all reasonable steps to ensure that:

- Students have access to necessary materials and resources
- Students know how and when they may contact the faculty member
- Students are aware of all relevant academic services available to them (particularly the library and information technology services)
- New students receive appropriate information on procedures, services, and personnel relevant to their introduction to the University and their continued studies

Termination of the Student Enrollment Agreement

The Student Enrollment Agreement will end automatically, subject to the student's rights of internal appeal, if the student's status in the University is terminated as a result of:

A. Action taken against the student in accordance with the University's disciplinary procedures
B. A decision of the faculty, based on the student's academic performance
C. Non-payment of fees, in accordance with the University's regulations on payment of fees.

In addition, the University may end this Agreement by written notice to the student in the following circumstances:

A. If, between accepting an offer and starting the program there is a change in the student's circumstances which, in the reasonable opinion of the University, makes it inappropriate for the student to begin the program

B. If the University becomes aware of information about a student which was not previously known (for example, criminal convictions) which, in the reasonable opinion of the University, makes it inappropriate for the student to begin the program

C. If, in the reasonable opinion of the University, the student has failed to provide the University with all relevant information or has supplied false or misleading information relating to the application for the program.

The date by which the notification is postmarked, phoned, or emailed is the effective date of the withdrawal. Any tuition or fees owed to the student will be refunded within 30 days of the receipt of the withdrawal notice.

All fees owed to the University are due immediately upon termination of the Enrollment Agreement. Accounts that have a negative balance will be sent to a 3rd party collection service.

Student Complaints and Grievances

EC-Council University provides a written procedure which details how students or other parties may register a complaint or grievance, how the institution will investigate the complaint, and how the institution will attempt to resolve the complaint.
The University is committed to handling any student complaint in a way which:

- encourages informal resolution
- is fair and efficient
- treats the student with appropriate seriousness and sympathy
- is quick and consistent with a fair and thorough investigation

The University defines a complaint as "a specific concern on the part of a student about the provision of education or other service by the University." Examples include but are not limited to:

- inaccurate or misleading information about programs of study
- inadequate teaching or supervision
- insufficient academic facilities
- service not provided to standard advertised
- the behavior of a member or staff
- the behavior of another student

If a student wishes to make a complaint, he or she must do so within 60 days of the date on which the event occurred.

A complaint may only be made by a student or group of students, not by a third party or a representative. Anonymous complaints will only be accepted if there is sufficient evidence to support it and will be treated with caution.

The student may have reservations about making a complaint, but the University takes complaints very seriously. Regulations provide that the student cannot be put at risk of disadvantage or discrimination as a result of making a complaint when the complaint has been made in good faith.

Students should note that all staff involved in a complaint will be required to respect the confidentiality of information and documents generated in, or as a result of, the complaint and not to disclose such information to people not concerned with the matters in question.

The hierarchy of complaints and grievances are typically as follows: 1) The person/department where the issue occurred, 2) The instructor (if any), 3) The Dean of Academic Affairs, 4) New Mexico Higher Education Department, and 5) The accreditation agencies where the institution holds accreditation. (More information on the following page.)

EC-Council University maintains open files for inspection regarding all complaints lodged within the past three (3) years against faculty, staff, and students.

EC-Council University encourages individuals to take the following steps when handling complaints:

Step 1
If possible, the complaint should be given to the individual directly responsible for the situation. EC-Council University will NOT take adversarial action against the student who lodged the complaint.

Step 2
If the student is dissatisfied or feels unable to confront the individual who is directly responsible, the student will need to notify the Dean of Academic Affairs at: Michael.Goldner@eccuni.us, who will investigate the matter and report back to the student with a solution within five (5) business days. The investigation will be handled in an impartial manner.

Should the student still be dissatisfied, he or she can seek relief from the New Mexico Higher Education Department at: New Mexico Higher Education Department, 2048 Galisteo, Santa Fe, NM 87505-2100, 1-505-476-8400 or http://hed.state.nm.us/Complaint.aspx.

From the NMHED website: "In accordance with the new Federal Program Integrity rules effective July 1, 2011, the New Mexico Higher Education Department (NMHED) will review complaints regarding public and private postsecondary institutions in New Mexico as well as New Mexico resident students attending out-of-state institutions."

Complaints not addressed can also be submitted to the Distance Education and Training Council (DETC) by completing the online complaint form at www.deac.org.

UNIVERSITY RIGHTS AND RESPONSIBILITIES

General

The University cannot accept responsibility, and expressly excludes liability, for:

- Any loss or damage to personal property and/or
- Death or any personal injury suffered by the student

Although the University will attempt to ensure that computer programs and software available for the student's use have reasonable security and anti-virus protections, the student should use such computer programs and software provided by the University at his or her own risk. The University will not be held liable for loss or damage suffered by the student or their property as a result of the use of any computer programs or software provided by or made available by the University, including any contamination of software or loss of files.

Neither the student nor the University will hold each other liable for failure or delay in performing obligations, if the failure or delay is due to causes beyond the party's reasonable control (e.g., fire, flood, or industrial dispute).

Third Parties

The parties to this Agreement do not intend that any of its terms will be enforceable by any person not a direct party to it.

Rights Reserved

EC-Council University reserves the right to add or delete from certain courses, programs, or areas of study as circumstances may require to enhance the quality and delivery of educational services. This includes but is not limited to: faculty changes, tuition rates, and fees. EC- Council University will give proper advanced notice in the event of any financial changes effecting students.

Student Records/Right of Privacy

Family Educational Rights and Privacy Act (FERPA) of 1974, as Amended

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their educational records.

- the right to inspect and review the student's educational records within 45 days of the day the University receives a request for access;
- the student's right to request the amendment of their educational records that the student believes are inaccurate or misleading;
- the right to consent to disclosures of personally identifiable information contained in the student's educational records, except to the extent that FERPA authorizes disclosures without consent.

1. Students should submit to the Registrar's office written requests that identify the records they wish to inspect. The University official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the University official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
2. Students may ask the University to amend records they believe are inaccurate or misleading. They should write the University official responsible for the record, clearly identifying the part of the record they want changed and specifying why it is inaccurate or misleading. If the University decides not to amend the record as requested by the student, the University will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.
3. Exceptions permitting disclosure without consent is to University officials* with legitimate educational interests. Other known person(s) and agencies are:
    - School officials with legitimate educational interest
    - Schools to which a student is transferring
    - Specified officials for audit or evaluation purposes
    - Appropriate parties in connection with financial aid to a student
    - Organizations conducting certain studies for or on behalf of the school
    - Accrediting organizations; a judicial order or lawfully issued subpoena
    - Appropriate officials in cases of health and safety emergencies.

*A University official has a legitimate educational interest if the official needs to review an educational record in order to fulfill his or her professional responsibility.

For more information on FERPA standards and guidelines that EC-Council University abides by, visit the US Department of Education at: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Directory Information

In compliance with the Family Educational Rights and Privacy Act (FERPA), the University treats the following student information as directory information, which can be disclosed without a specific release of information from the student: name, field of study, degrees/ awards, participation in officially recognized activities, dates of attendance, and level of enrollment.

Students may restrict the release of directory information by written request available from the Director of Admissions/Registrar at registrar@eccu.edu.

Non-Directory Information

In compliance with FERPA guidelines, a student must provide self- identifying information in a signed and dated written request to the Registrar for the release of non-directory information. The receipt of a written request by fax satisfies this requirement.

Electronic Files

The Family Educational Rights and Privacy Act (FERPA) does not differentiate between the medium of storage or the method of transmission. There is no legal difference between the level of protection afforded to physical files over those that are stored or transmitted electronically or in any other form.

Access to Records

Any currently enrolled or former student has a right of access to any and all records relating to the student and maintained by the University. Individuals who applied to the school but did not attend are not covered by FERPA. The full policy and procedure for review of a student's records are available from the Registrar.

- Students 18 years of age or older may examine all records in their name. These records are not available to any other person other than appropriate University personnel, unless released by the student. Legal exception is provided to the above regulation, and these exceptions will be explained to any person who requests the information from the Director of Admissions and Registrar.
- Each student has a right to challenge any record, which is kept by the University. The Director of Admissions and Registrar is responsible for all student records. Challenge of records, if any, shall be in writing to the Registrar at registrar@eccuni.edu. A decision will be made within five business days to uphold or reject the challenge of any record. When the challenge of a record is upheld, the record shall be amended. If the challenge of a record is denied, the student may appeal this decision to the Dean.
- The specific regulations governing the Family Educational Rights and Privacy Act are available in the office of the Dean and the office of the Registrar.

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

Family Policy Compliance Office
U.S. Department of Education 400 Maryland Avenue, S.W. Washington, DC 20202-4605Disability

Disability

The University uses the definition of disability set forth in Section 504 of the Rehabilitation Act of 1973, which states that a disabled person is anyone who:

- has a physical or mental impairment which substantially limits one or more major life activities;
- has a record of such impairment;
- is regarded as having such impairment.

In order to receive accommodations, the student must meet the following criteria:

- has a documented disability (documentation must be supplied) that presents a significant barrier to the educational process, and
- request services from a faculty member or ECCU's administrative staff.

Students are required to provide the professional staff counselor with medical or psychological documentation in order to receive accommodations. All medical information remains confidential and is only released to other University personnel with the student's written permission.

Student Rights

EC-Council University encourages diversity within its student body and strives to provide its students with a secure and safe environment conducive to learning. The student's rights consist of the following but are not limited to:

- Students will have the web course materials they need to complete assignments and to participate in group or class sessions. This support may be achieved with one or a combination of the following: courier, overnight delivery (FedEx, UPS, and Express Mail), priority mail, electronic file transfer, and fax. With a long lead time, regular mail service may be an alternative.
- EC-Council University ensures that all students will be treated equally.
- EC-Council University will make available the necessary services for required proctored examinations, however the cost of these services will be borne by the student.

Anti-Harassment

EC-Council University does not tolerate any form of harassment, sexual misconduct, or inappropriate behavior by students, faculty, instructors, or University staff. Anyone who believes that he or she is the recipient of such behavior must immediately contact the President with a written account and details of the incident(s) so that an appropriate investigation can be made. All communications will be held in the strictest confidence, and the constitutional rights of the individuals involved will be protected.

Non-Discrimination

The University is in compliance with all requirements imposed by or pursuant to Title VI for the Civil Rights Act of 1964 and Section 504 of the Rehabilitation Act of 1973. The institution does not discriminate on the basis of race, sex, color, creed, age, religion or national origin in its admissions, activities, programs, or employment policies in accordance with federal, state, and local laws.

PROGRAM COSTS AND PAYMENT

It is the responsibility of the student to ensure tuition, fees, and all other expenses relating to the program are paid. The tuition and fee amounts are made available to the student on the University website www.eccu.edu, prior to each term and are subject to review and revision each academic year. The student is bound by the University's regulations on the payment of tuition and fees, the refund of tuition in the event of termination of the student's studies, and the consequences of non-payment.

Undergraduate tuition

Application fee	$75

Tuition:*

Region 1	$398 /credit hour	**Region 2**	$330 /credit hour	**Region 3**	$263 /credit hour

Proctor Now	$15 per exam (5 Required)
Graduation fee	$100
Other fees:	
Transcript fee	$10+shipping**
Transcript w/Apostille	$20+shipping**

Total Bachelor of Security in Cyber Security Program Price (estimated)

The total cost estimate is based on completing 60 credit hours with tuition rates, applied based on the geographical region, of the student plus required fees. To be considered full time in Bachelor Science in Cyber Security students must be enrolled and complete 6 courses per term.

Additional cost may be incurred by the student with the purchase of textbooks, shipping, electronic equipment, connectivity charges and exam proctoring.

Region 1	$24,130 + books	**Region 2**	$20,050 + books	**Region 3**	$16,030 + books

*While many textbooks are available online through Aspen and LIRN, students may elect to purchase textbooks. Depending on the course choices students make, they can expect to spend between $250 and $900 USD for textbooks.

**There is no charge for shipping to students residing in the United States if using ground US Postal Service. Expedited shipping is available for an additional charge.

Graduate tuition

Application fee $75

Tuition: *

Region 1
$473 per credit hour

Region 2
$405 per credit hour

Region 3
$338 per credit hour

Lab fees
$50
(3 Required)

Proctor Now
$15 per exam
(5 Required)

Graduation fee
$100

Other fees:

Transcript fee	$10+shipping**
Transcript w/Apostille	$20+shipping**

Total Master of Science in Cyber Security Program Price (estimated)

The total cost estimate is based on completing 36 credit hours with tuition rates applied based on the geographical region of the student plus required fees. Fees include application fee, proctor fee (5), lab fee (3), and graduation fee.

To be considered full time students must be enrolled and complete 3 courses per term for the Master of Science in Cyber Security.

Additional cost may be incurred by the student with the purchase of textbooks, shipping, electronic equipment, connectivity charges and exam proctoring.

Region 1	$17,428 + books
Region 2	$14,980 + books
Region 3	$12,568 + books

*Most textbooks are embedded digitally in courses, students may elect to purchase textbooks. Depending on the course choices students make, they can expect to spend between $250 and $900 USD for textbooks.

**There is no charge for shipping to students residing in the United States if using ground US Postal Service. Expedited shipping is available for an additional charge.

Total Graduate Certificate Program Price (estimated)

Graduate Certificates:

Information Security Professional

Region 1	$4497+ books	**Region 2**	$3885 + books	**Region 3**	$3282+ books

It Analyst

Region 1	$4547 + books	**Region 2**	$3935 + books	**Region 3**	$3332 + books

Digital Forensics

Region 1	$4497+ books	**Region 2**	$3885 + books	**Region 3**	$3282+ books

Disaster Recovery

Region 1	$4547 + books	**Region 2**	$3935 + books	**Region 3**	$3332 + books

Executive Leadership in Information Assurance

Region 1	$4447 + books	**Region 2**	$3835 + books	**Region 3**	$3232 + books

This includes:

Application fee $75	Tuition - 9 credit hours	Lab fees (varies by program, 0-$100)	Proctor exam fee $15	Graduation fee $100	Students will also receive an EC-Council Exam Voucher

Cyber Security Professional	CEH or ENSA	It Analyst	EDRP	Digital Forensics	CHFI
Disaster Recovery	ECSA or EDRP	Executive Leadership in Cyber Security	none		

Explanation of Regions

Regions have been defined by the ECCU Governing Board. Student tuition rates are based on their official government photo ID that was submitted with the student admission application.

Region 1: Algeria, Australia, Austria, Belgium, Canada, Croatia, Cyprus, Denmark, France, Germany, Greece, Hungary, Ireland, Italy, Kingdom of Saudi Arabia, Korea, Kuwait, Malta, Mexico, Netherlands, New Zealand, Oman, Poland, Portugal, Qatar, Singapore, Slovenia, Spain, Sweden, Switzerland, United Arab Emeritus, United Kingdom, and United States of America.

Region 2: Bahrain, Cambodia, Estonia, Hong Kong, Indonesia, Japan, Jordan, Latvia, Lebanon, Lithuania, Macedonia, Malaysia, Mexico, Philippines, Taiwan, Thailand, and Vietnam.

Region 3: All of Africa, India, Central and South America.

Fees

Application Fee $75 (Program Fee)
The application fee covers the administrative cost associated with processing an application. An application is not considered complete without the accompanying, one-time, non-refundable application fee. (Insert verbiage explaining if, when and why this fee would ever be waived.)

Tuition (Course Fee/ credit hour)
Masters Program: Region 1- $473/ credit hour; Region 2- $405/ credit hour; Region 3- $338/ credit hour
Bachelors Program: Region 1- $398/ credit hour; Region 2- $330/ credit hour; Region 3- $263/ credit hour

Lab Fee $50 (Course Fee) ECCU 501, 502, 503, 506, 513
All graduate courses accompanied by a lab will be assessed a lab fee of $50.

Remote Proctor Now Exams ($15 per exam)
Some courses may require a proctored exam. Payment for a proctored exam is the responsibility of the student. Students will be notified in the course syllabus by the instructor if this fee is applicable to the course.

Graduation Fee $100
A Graduation Fee of $100 is due at the time a student is in the final term of their degree and submits the graduation application to the Registrar. The Registrar will verify the student has completed all necessary requirements for graduation, including payment of the graduation fee. The Registrar will approve the graduation request form and submit it to the Dean. Once the Dean verifies a student's graduation application, the earned degree will be conferred and sent along with two (2) official and one (1) unofficial transcript with a congratulatory letter, degree, and memorabilia in the graduation packet.

Tuition costs are payable in USD.

Students outside the United States may inquire about program cost at info@eccu.edu or by calling 1-505-922-2889.

Refund Policy

Tuition refunds are paid when a student pre-pays a portion or all of the tuition for a course or program and then withdraws from the course or program prior to the predetermined deadline. Tuition refunds are made within 30 days of notice of withdrawal. Refunds may also be applied to the cost of future courses. The student is notified if a balance is due to the University. Tuition refunds are based on the following schedule and policies:

Five day cooling off period

The student has five days after signing the enrollment agreement to cancel the agreement and receive a full refund of all monies paid.
Student notification of cancellation may be conveyed to ECCU in any manner.

After the five day cooling off period

Refunds are calculated on a per class basis. If a student withdraws during their first term, a registration fee of $200 will be charged. The registration fee is deducted prior to calculating the refund.

Percentage of tuition refunded to the student minus the registration fee is based on the following schedule:

Week Withdrawn	% refunded
1st week	80%
2nd week	70%
3rd week	60%
4th week	50%
5th week	40%
6th week	30%
7th week	20%
8th week	10%
9th - 12th week	0%

All refunds are calculated in USD. All refunds are based on the amount of tuition and lab fees paid less scholarships or fellowships. The University will refund 100% of any monies received for the overpayment or pre-payment of future courses.

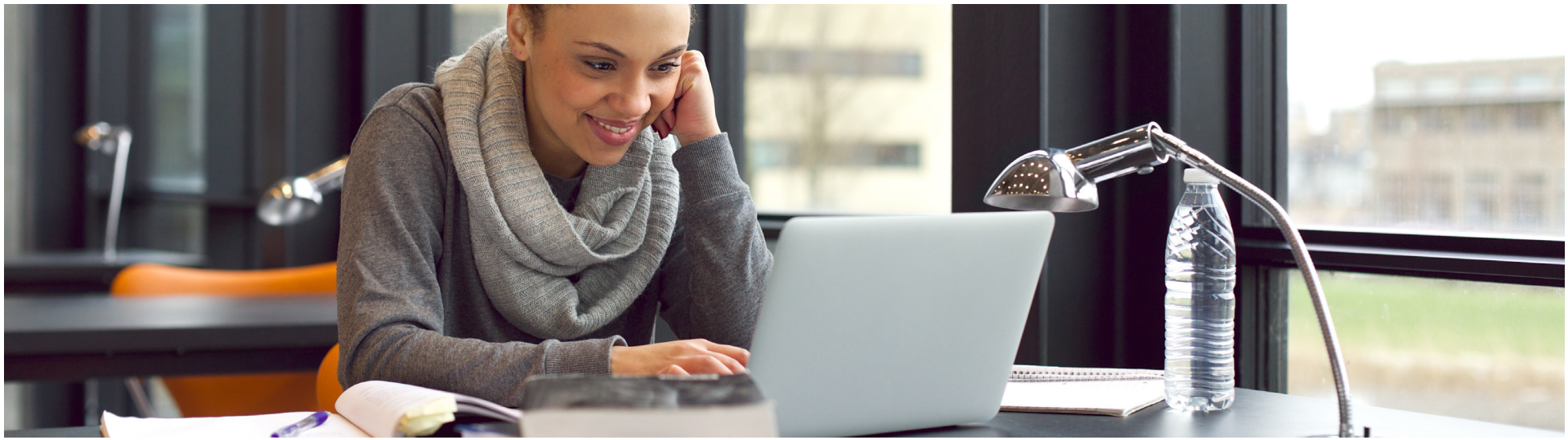
Examples (in USD):

a. Bob returned his enrollment agreement and paid Region 1 tuition for a 3-credit class with a lab fee, totaling $1,469. Three days later he withdrew from the cyber security program. He received a full refund of $1,469, because he withdrew during the "5 day cooling off period"

b. Sally returned her enrollment agreement and paid region 1 tuition for a 3-credit class with a lab fee, totaling $1,469. The day before classes began she withdrew from the class. Prior to the beginning of class during a student's first term, students receive a refund of the tuition less the $200 registration fee. Sally received a refund of $1,269.

c. Mohamed returned his enrollment agreement, paid Region 1 tuition for a three-credit class with a lab, totaling $1,469. During the third week he withdrew from the class. In week 3 of class during a student's first term, students receive a refund of 60% of the tuition after deducting the $200 registration fee. Mohamed received a refund of $761.74.

d. Elvis was in his second term of classes. He paid Region 1 tuition for a 3-credit class with a lab, totaling $1,469. During the third week he withdrew from the class. In week 3 students receive a refund of 60% of the tuition. He was not charged the registration fee because this was not his first term of classes. Elvis received a refund of $881.40



Special Circumstances

In the case of a student's illness, accident, death in the family, or other circumstance beyond the control of the student, the student may be entitled to special consideration for extenuating situations; The University may settle the account for a lesser amount than the amount required by the established policy. To be considered for special circumstances, the student should contact the Director of Admissions/Registrar.

EC-Council University Board of Directors

Sanjay Bavisi,
Chairman President and CEO of EC-Council
LLB (Hons), Middle Temple [United Kingdom]

Allan Berg,
Master of Education,
The American University
Bachelor of Science, Towson State University

Dr. Sharon Caballero,
Ed.D. and Master of Arts, US International University;
Bachelor of Arts, San Diego State University

Michael Tamasi,
Master Business Administration, Western Governor's University;
Bachelor of Science, Western Governor's University

Dr. David Ward,
Ph.D. Capitol College; JD,
Pace University School of Law;
MS Pepperdine University;
BA Queen's College, City University of New York

Joan Franklin,
Ph.D Doctor of Philosophy, Management and Andragogy, Texas Womans University; Master of Education, Counseling Psychology, Texas Woman's University; Bachelor of Arts, Texas Woman's University.

EC-Council University Advisory Council

Charlie Cayott

Polytechnic University
MS-ISE, Information Systems Engineering

Regents College - SUNY
BS, Business, Sociology, Political Science

Rockland Community College
AAS, Business, Psychology

Dr. Marcy Sylvester Ceranek

Nova Southeastern University
Ed.D., Higher Educational Leadership,

Northern Illinois University
M.B.A., Management

Augustana College
B.A., Accounting and Business Administration (Management)

Stephen Miller

Houston Baptist University
MS/MIS Managing Computer Technology

University of Houston
BS/BIS Business Services

EC-Council University Staff

Dr. Randy Plunkett,
University Dean
Education Leadership Doctorate, Wilmington University, New Castle DE;
Master of Science,Marian University Fond Du Lac, WI Bachelor of Science, Maranatha Baptist Bible College Watertown, WI

Nancy Speisser
Master of Library Science, The Catholic University of America
Bachelor of Arts in Management, Virginia Weslean College

Nicole McFarling
Manager of Student Services/Registrar
PhD candidate Special Education, University of New Mexico
Master of Arts, Special Education, University of New Mexico
Bachelor of Arts, English, San Jose State University

Kathy Liebhaber
Office Administrator

David Valdez
Recruiting and Outreach Specialist

Faculty

Dominic Boamah
Adjunt Faculty
Doctor of Philosophy degree (Ph.D.) with emphasis on Information Technology Management, Capella University, Master of Science degree in Information Systems, University of Jyvaskyla, Finland

Yuri Diogenes, MS
Adjunct Faculty
Master of Science in Cybersecurity Intelligence and Forensics Investigation from UTICA College; MBA from FGV Brazil. CISSP, E|CEH, E|CSA, CompTIA, Security+, CompTIA Cloud Essentials Certified, CompTIA Mobility+, CompTIA Network+, CompTIA Cloud+, CASP, MCSE and MCTS.

Matthew Vogel
Adjunct Faculty
Associate of Arts in General Studies, City Colleges, Bachelors of Arts in Information Systems Management, University of Maryland, Masters of Science in Management Information Systems, University of Phoenix

Sandro Tuccinardi
Adjunct Faculty
Juris Doctorate, McGill University;
Master of Science, Computer Science, Dalhousie University;
Bachelor of Arts, Social Science, University of Ottawa

Arnold Webster
Adjunct Faculty
Master of Science, Network Security, Capitol College, Laurel, Maryland;
Bachelor of Science, City University, Bellevue, Washington

Yakov Goldberg
Adjunct Faculty
Bachelor of Science, ITT Technical Institute;
Master of Science, Capella University

Joan Franklin, Ph.D
Adjunct Faculty
Doctor of Philosophy, Management and Andragogy, Texas Womans University;
Master of Education, Counseling Psychology, Texas Woman's University;
Bachelor of Arts, Texas Woman's University

Georgia Brown, MS
Adjunct Faculty
Master of Science in Information Technology, Strayer University; Bachelor of Science in Computer Information Systems, Excelsior College.

Danielle Babb
Adjunct Faculty
PhD in Organization and Management, Information Technology Management specialization, Capella University, Masters of Business Administration, Information Systems Emphasis, University of Redlands, Bachelor of Science, Business Administration, University of California at Riverside.

Julie Phillips
Adjunct Faculty
Ph.D., Professional Studies in Education, Capella University, Minneapolis, MN M.S., Psychology, Capella University, Minneapolis, MN B.S., Social Psychology, Park University, Parkville, MO

Pamela Garrett
Adjunct Faculty
MBA, Concentration in Supply Chain Management, Strayer University; Master of Engineering Management Old Dominion University; Bachelor of Science, Industrial Engineering, Louisiana State University. PE, Professional Engineer Licensed in Virginia

Linda Walters
Adjunct Faculty
Master of Science Computer Science, Norfolk State University; Bachelors Business Administration in Information Systems, Monroe College

Willie Session
Adjunct Faculty
Applicant: Doctorate of Philosophy: Public Policy and Administration, Walden University; Master Business Administration, National University; Bachelor of Science, Southern Illinois University

Chanel Suggs
Doctoral candidate with an emphasis in Cyber security. Master of Science in Cyber Security, Capital College; Master in Networking and Communications with concentration in Cyber Security, Keller Graduate University; MBA; Keller Graduate University; Bachelor of Science in Computer Science with a minor in Psychology, University of North Carolina

Copyright

EC-Council University follows the copyright law of the United States which prohibits the making or reproduction of copyrighted materials except under certain specified conditions. Acts of copyright infringement include, but are not limited to, misusing copyrighted material in one's coursework and misusing material for which the institution owns the copyright (i.e., web site materials, course materials, publications, etc.). Copyright infringements involving students and/or employees of EC-Council University may be subject to the disciplinary action including, but not limited to, dismissal from the University.

The Catalog

This catalog articulates the regulations, policies, programs and procedures for the University and applies to students enrolled between Jan 1, 2017 and December 31, 2017. Students inactive (not enrolled) for one calendar year must be readmitted and will move forward to the catalog current at the time of their readmission. The catalog is not to be construed as a contract between the student and the University. Not all of the images contained in this catalog are ECCU faculty, staff or students, but they represent the wide diversity of the faculty, staff and students at ECCU. The ECCU Student Enrollment Agreement includes the terms and conditions of attendance at the University. The University reserves the right to change/edit the contents of the catalog as it deems appropriate at any time by means of producing a catalog addendum.

EC-COUNCIL
UNIVERSITY

EC-Council University 101 C Sun Ave NE Albuquerque, NM 87109

 info@eccu.edu

 www.eccu.edu

 1-505-922-2889

 1-505-856-8267