EC-COUNCIL
UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

The Leader in Cyber Security Education

2021 Catalog

Effective March 21, 2021

Version 2021 2.0

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAIRMAN'S MESSAGE

JAY BAVISI
Chairman of the Board
of EC-Council University

Dear 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
Chairman of the Board of EC-Council University

THE UNIVERSITY

Mission Statement

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

INSTITUTIONAL GOALS AND OBJECTIVES

Strive to strengthen Institutional effectiveness and collegial governance

- Promoting and encouraging continuous learning and support
- Fostering collaboration among 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
- Implementing iLabs for student engagement
- Promoting cybersecurity educational programs and webinars at no cost to the public
- Preparing our students to be socially responsible in Cyber Security leadership roles

THE UNIVERSITY

Provide a supportive and welcoming environment to a diverse academic community

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

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 cybersecurity professionals. Cybersecurity 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 cybersecurity certifications used throughout the globe, is the parent company of EC-Council University. EC-Council University Chairman of the Board Sanjay Bavisi believes that cybersecurity 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 and Bachelor of Science in Cyber Security program.

Institutional Values

ECCU places particular value on the qualities of ethical behavior, innovative thinking, critical thinking, leadership, and students. In a field as narrow and yet far-reaching as cybersecurity, these values promote and advance the ultimate goal of educating cybersecurity 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 multidimensional 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 2044 Galisteo Street, Suite 4, Santa Fe, New Mexico, USA, 87505-2100, 505-476-8400.

CNSS Standards

ECCU courseware for ECCU 500 (CNSS 4011), ECCU 501 (CNSS 4013A), ECCU 502 (CNSS4012), ECCU 503 (CNSS 4014), ECCU 506 (CNSS 4015), and ECCU 513 (CNSS4016) are mapped to the former Committee on National Security Standards (CNSS).

NATIONAL INSTITUTE OF STANDARDS & 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 essential aspects of cybersecurity workforce planning is identifying the workforce and various 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, CIS408, ECCU 500, ECCU 501, ECCU 502, ECCU 503, and ECCU 510 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).

ACCREDITATION

Accredited by the Distance Education Accrediting Commission

Address: 1101 17th Street NW, Suite 808 Washington, DC 20036 | Phone: (202) 234-5100 | Website: www.deac.org

The Distance Education Accrediting Commission is listed by the U.S. Department of Education as a recognized accrediting agency. The Distance Education Accrediting Commission is recognized by the Council for Higher Education Accreditation (CHEA).

DEAC
DISTANCE EDUCATION ACCREDITING COMMISSION

CHEA
Council for Higher Education Accreditation

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

Phone:
(505) 922-2886

Fax:
(505) 856-8267

Website:
www.eccu.edu

Mailing Address:
101-C Sun Ave NE
Albuquerque, NM 87109

Contact Us By Department

Student Services & Registrar

Email: registrar@eccu.edu

Phone: (505) 922-2886

Enrollment & Advising Specialist

Email: info@eccu.edu

Phone: (505) 796-8214

Office & Finance Administrator

Email: finance@eccu.edu

Phone: 505-922-2889

Complaints & Grievances

Email: registrar@eccu.edu

ACADEMIC CALENDAR

DATES AND DEADLINES

Term	Term Start Date	Term End Date	Registration Begins	Registration Ends	Payment Deadline	Last Day To Withdraw With a W	Last Day To Withdraw With Approval
Term 3	July 6, 2020	September 27, 2020	May 15, 2020	July 5, 2020	July 16, 2020	September 13, 2020	September 20, 2020
Term 4	October 5, 2020	December 27, 2020	August 15, 2020	October 4, 2020	October 15, 2020	December 13, 2020	December 20, 2020
Term 1	January 4, 2021	March 28, 2021	November 15, 2020	January 3, 2021	January 15, 2021	March 14, 2021	March 21, 2021
Term 2	April 5, 2021	June 27, 2021	February 15, 2021	April 4, 2021	April 15, 2021	June 13, 2021	June 20, 2021
Term 3	July 5, 2021	September 26, 2021	May 15, 2021	July 4, 2021	July 15, 2021	September 12, 2021	September 19, 2021
Term 4	October 4, 2021	December 26, 2021	August 16, 2021	October 3, 2021	October 15, 2021	December 12, 2021	December 19 2021

2020-21 HOLIDAYS

Holiday	2020	2021	Holiday	2020	2021
New Year's	January 1	January 1	Labor Day	September 7	September 6
Martin Luther King	January 21	January 18	Columbus Day	October 12	October 11
President's Day	February 17	February 15	Veteran's Day Observed	November 11	November 11
Memorial Day	May 25	May 31	Thanksgiving Holiday	November 26-27	November 25-26
Independence Day	July 3 (Observed)	July 5 (Observed)	Winter Break	December 24-25 December 31-January 1 2021	December 23-26 December 31-January 1, 2022

STUDENT SERVICES

International Student Admission and Visa Services

The University does not provide any immigration status sponsorship or any 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.

Scholarship Opportunities

Please see page 82 for more details.

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 issued a login for Populi and Canvas. 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 can interact with an Academic Advisor 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 8 am-4 pm MST. Instructor virtual office hours are posted on the course syllabus.

Students have access to private 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. Also, students have access to the online library and a database search engine (LIRN).

ADMISSION REQUIREMENTS

Application Procedure

Applicants with a degree from a US institution

Prospective students wishing to attend EC-Council University shall submit a complete application package, including a signed Student Enrollment Agreement (SEA) form (available online at http://www.eccu.edu/student- services/admission/) that lists all prior institutions attended with the application fee. Please see the section titled Required Documents for the full application package requirements.

Prospective students must provide official transcripts for evaluation of transfer credits before an official decision on admission is made. A copy of your unofficial transcripts may be submitted for provisional admission, but for full admission, an official copy must be submitted.

Official transcripts need to be sent to:

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

Applicants with a degree from a Non-US institution

In addition to the above requirements, applicants with degrees from other than US institutions must provide proof of the US equivalency of their foreign degree. In order to have a degree from a non-US institution evaluated, applicants must submit unofficial transcripts for all degrees earned to EC-Council University. EC-Council University will send the copies of your transcript to be evaluated by an independent evaluator appointed by the University for a fee of $115 USD. ECCU will also accept an evaluation of the transcripts completed by an authorized globally recognized agency. The transcripts must include a list of all classes completed and grades awarded.

Prospective students will need to contact the University where they earned their degree and request that the official transcript and other official documentation be sent to 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.

Students also have the option of utilizing ECCU's NAFSA evaluation servicer, Strategy Consultants. Transcripts can be evaluated for a fee of $115. Documents can be translated for an additional fee upon request. Please contact your Enrollment Advisor for more information.

Official transcripts need to be sent to:

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

ADMISSION REQUIREMENTS

Admission

Following submission and acceptance of the Student Enrollment Agreement (SEA), a student may be fully, provisionally, or conditionally admitted to ECCU.

» **Fully admitted**
Students will be fully admitted to the university following receipt of all official documents required for admission and upon meeting all requirements for admission.

» **Provisionally admitted**
Students who have not submitted all the official documents required for full admission (such as official transcripts) will be provisionally admitted to the university pending receipt of the official documents. By the end of the first term, all official documents required for full admission must be submitted. If by the end of the first term we do not receive all required documents, students will be placed on a registration lock. This may result in the delay of full admission, denial of admission, or administrative withdrawal from ECCU.

» **Conditionally admitted**
Students who do not meet all the requirements for admission (for example, GPA less than the required minimum) may be conditionally admitted to ECCU upon approval of an admission appeal by the applicant to the Dean provided that all official transcripts and documents required for admission have been submitted to EC-Council University. See Admission Appeals for more information. Conditional admission will be revoked if the student fails to meet Satisfactory Academic Progress or other admissions or academic standards that have been approved as conditions for admission.

Students are also required to review and sign the Student Enrollment Agreement (SEA) form as part of the admission process.

Admission Appeals

Prospective students who do not meet admission requirements may appeal the admissions decision to the Dean. Before the Dean's review, the student should submit a personal statement for consideration in making the decision. Those students whose appeal is successful will be admitted with conditions as set forth by the Dean.

ADMISSION REQUIREMENTS

Admission Is Not Guaranteed

Full admission to the university is predicated upon students' submission and the university acceptance of all official documents required for admissions. Prospective students acknowledge that just because they have submitted an application or unofficial transcripts or have been enrolled in a course under provisional admission, that their full admission to the university is not guaranteed.

It is the student's responsibility to provide all the information required for admission to the university, including clearing any holds placed on transcripts from previous universities attended. Students who do not submit all official documents by the end of their first term will be put on an enrollment hold pending their submission and acceptance and may result in their being denied admission to the university.

EC-Council University reserves the right to refuse or revoke admission to the University if:

- The prospective student does not meet the University's requirements for admission.
- There are discrepancies to the provided admission documents that cannot be resolved, including false or missing information.
- The student is a threat or disruptive to the University's community or its operations, including breach of EC-Council University's code of ethics and/or other inappropriate actions.

ENGLISH REQUIREMENT

There are several ways to show proof that you meet the English requirement.

» If your degree is earned in a country where English is the official language, you do not need to provide additional proof. For example, if your degree was earned in the Anguilla, Antigua and Barbuda, Australia, Bahamas, Barbados, Belize, Bermuda, Botswana, British Virgin Islands, Cameroon, Canada (except Quebec), Cayman Islands, Dominica, England, Fiji, Gambia, Ghana, Gibraltar, Grenada, Guyana, Ireland (Northern and Republic of), Jamaica, Kenya, Lesotho, Liberia, Malawi, Malta, Mauritius, Montserrat, Namibia, New Zealand, Nigeria, Papua New Guinea, St. Kitts and Nevis, St, Lucia, St. Vincent and the Grenadines, Scotland, Seychelles, Sierra Leon, Singapore, Solomon Islands, South Africa, Swaziland, Tanzania, Tonga, Trinidad and Tobago, Turks and Caicos Islands, Uganda, United Kingdom, Vanuatu, Wales, Zambia, or Zimbabwe.

» If English was the language of instruction at the university where you earned your degree, then you must provide a letter from the institution stating that English was the language of instruction. Or you can also request that the NACES, NAFSA or evaluator appointed by the university states the language of instruction on the degree evaluation.

» You can show English proficiency by taking a recognized English proficiency test.

Present official documents with an appropriate minimum total score for one of the following exams:

Degree Level	TOEFL Internet-Based Test (IBT)	TOEFL Paper- Based Test (PBT)	IELTS
Undergraduate	61+	500+	6.0+
Graduate	71+	550+	6.5+

TECHNOLOGY REQUIREMENTS

To benefit from the unique features that ECCU provides, students will need to possess or have access to a computer with the following:

Personal computer with Windows Operating System

» **Chrome OS is not supported by ProctorU**

Standard Web browser like Microsoft Edge, Firefox, or Chrome

Microsoft Office applications, including, at a minimum: PowerPoint, Word, and Excel

Adobe PDF reader

Webcam

Internet connectivity

Headphones with microphone (required in some programs)

PROGRAM ADMISSION REQUIREMENTS

Admission Requirements

The following admission requirements apply:

Bachelor's Degree Programs

Students requesting admission to undergraduate degree programs shall:

» 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), of which 25% must be general education credits.

» Submit proof of High School Diploma or foreign equivalent OR have an earned degree of an associate's degree or higher

» 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

» Demonstrate proof of English proficiency (international students only; see the section on English Requirements for International Students)

Master's and Graduate Certificate Programs

» 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 minimum CGPA of 2.5 on the transcript of the most recently conferred bachelor's or master's degree for full admission
» Proof of English proficiency (international stduents only; see the section on English Requirement for International Students)

Non-Degree Status

Students looking to improve their professional or personal development without having to fulfill degree requirements are welcome to apply as non- degree students. The Non-Degree Status is designed for scholars from across the world looking to take a specific course or course from ECCU's Bachelor's or master's degree programs. A maximum of two courses (6 credits) may be taken in non-degree status or three courses (9 credits) by Prior Learning Assessment transfer.

PROGRAM ADMISSION REQUIREMENTS

Admission Requirements for Non-Degree Status

To qualify for a course with non-degree status, applicants must:

» Be 18 years of age or older
» Have earned and submitted proof of high school diploma or equivalent, or college degree or certification

Required Admission Documents

The following documents are required for admission:

Bachelor's Degree Seeking Students

» Be 18 years of age or older
» Student Enrollment Agreement
» Official government ID or passport (international students)
» A photo of yourself (selfie) holding your official government ID
» Official transcript(s) of all prior academic work
» Official evaluation of international credits (for students with international transcripts only)
» Proof of High School Diploma or foreign equivalent OR have an earned degree of an associate's degree or higher
» Proof of completion of 60+ semester credit hours (90+ quarter credit hours) or foreign equivalent
» Proof of English proficiency (international students only; see the section on English Requirement for International Students)
» Application Fee

Master's Degree Seeking Students

» Be 18 years of age or older
» Completed Students Enrollment Agreement
» Official government ID or passport (international student)
» A photo of yourself (selfie) holding your official government ID
» Official transcript(s) from the institution where the student received a bachelor's or most recent master's degree.
» Official evaluation of international credits (for students with international transcripts only)
» Proof of English proficiency (international students only; see the section on English Requirement for International Students)
» Application fee

Military Students

» LES or DD 214 (if separated from the military)
» VA Certificate of Eligibility (COE)
» Transfer of Program Form (if transferring student)
» Joint services transcripts
» Any additional transcripts from accredited academic institutions

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 academic cybersecurity credits) must have been earned within the last ten 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 for the master's and Graduate Certificate Programs. All course transfer credits for the bachelor's program must be a C or better.

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 maximum transfer credit of 18 graduate credit hours towards a master's degree and 30 undergraduate credit hours to the required 60 credits for admission for a total of 90 credit hours in a bachelor's degree.

Transfer credits are not considered in the calculation of the student's ECCU cumulative GPA.

Transfer credits accepted will count for both attempted and completed credits for the Satisfactory Academic Progress calculation of pace of completion (Percentage of Credit Completion - PCC).

All transfer credits must map to ECCU program course requirements to be utilized as transfer credit. General education course requirements are 25% of the total transfer credit and the total of the undergraduate program requirements. Minimum Math and English requirements are considered a part of the General Education requirement for undergraduate students. EC-Council University may also accept transfer credits from military and other non-traditional sources such as credits recommended by American Council on Education (ACE) or National College Credit Recommendation Service (NCCRS) as well as other sources may be considered; all non-traditional credits will be considered on a case by case basis.

Prior Learning Assessment

As a prospective EC-Council University student, you may be awarded appropriate credit for your demonstrated knowledge gained from industry certifications. To request credit, based on industry certifications, you are required to provide documentation of the certificates for the course(s) for which you are seeking credit. Credit for industry certificates is awarded based on an assessment by ECCU administrative team. Certifications must not be older than one year past the expiration date. Certifications can only be used in one program, e.g., if a student started in the Bachelor's program and transferred in their CEH (Certified Ethical Hacker) to apply for the CIS 404 Course. After completing their BSCS degree, the student wants to complete their MSCS degree; they cannot use the CEH and transfer it in for the ECCU 501 (Master's equivalent) course.

There is a Prior Learning Assessment fee of $50 per credit hour for non-degree students.

Submit all supporting documents to registrar@eccu.edu. You will be notified of what, if any, credit you will receive and how it will apply to your degree plan.

TRANSFERRING CREDIT

Below are standard industry certifications accepted for transfer credit:

Industry Certification	*Certifying Body*	*BS Course Equivalent*	*MS Course Equivalent*	*Credits*
AWS Certification (Associate or Professional)	Amazon	N/A	ECCU 525	3
CCENT (Cisco Certified Entry Networking Tech)	Cisco	CIS 403	ECCU 500	3
CCNA (Cisco Certified Network Associate)	Cisco	CIS 403	ECCU 500	3
CCNP (Cisco Certified Network Professional)	Cisco	CIS 403	ECCU 500	3
CASP +	CompTIA	CIS 403	ECCU 500	3
CompTIA A +	CompTIA	CIS 403	ECCU 500	3
Linux +	CompTIA	CIS 402	ECCU 507	3
PenTest +	CompTIA	CIS 404	ECCU 501	3
Security +	CompTIA	CIS 303	N/A	3
Network+ and Security + (must have both)	CompTIA	CIS 403	ECCU 500	3
C|EH (Certified Ethical Hacker)	EC-Council	CIS 404	ECCU 501	3
CHFI (Computer Hacking Forensics Investigator)	EC-Council	CIS 406	ECCU 502	3
CND (Certified Network Defender)	EC-Council	CIS 403	ECCU 500	3
ECIH	EC-Council	N/A	ECCU 522	3
ECSA	EC-Council	N/A	ECCU 503	3
EDRP	EC-Council	N/A	ECCU 513	3
EISM/CCISO	EC-Council	N/A	ECCU 523	3
LPT Master	EC-Council	N/A	ECCU 506	3
CFCE (Certified Forensic Computer Examiner)	IACIS	CIS 406	ECCU 502	3
CISA (Certified Information Security Auditor)	ISACA	N/A	ECCU 511	3
CISM (Certified Information Security Manager)	ISACA	N/A	ECCU 514	3
CCFP (Certified Cyber Forensics Professional)	ISC^2	CIS 406	ECCU 502	3
CISSP (Certified Info System Sec Professional)	ISC^2	CIS 404	ECCU 511	3
SSCP (Systems Security Certified Practitioner)	ISC^2	CIS 406	ECCU 502	3
MCSA (Microsoft Certified Solutions Associate)	Microsoft	CIS 403	ECCU 500	3
MCSE (Microsoft Certified Solutions Expert)	Microsoft	CIS 403	ECCU 500	3
CAPM (Certified Associate in Project Management)	PMI	MGT 450	ECCU 515	3
PMP (Project Management Professional)	PMI	MGT 450	ECCU 515	3
GCED (Certified Enterprise Defender)	SANS	CIS 404	ECCU 501	3
GCFA (GIAC Certified Forensic Analyst)	SANS	CIS 406	ECCU 502	3
GCIH (Certified Incident Handler)	SANS	N/A	ECCU 522	3
GPEN (GIAC Penetration Testing)	SANS	CIS 404	ECCU 503	3
GSEC (Security Essentials Certification)	SANS	CIS 403	ECCU 500	3
GSNA (Systems and Network Auditor)	SANS	CIS 403	ECCU 500	3

TRANSFERRING CREDIT

Maximum Allowable Transfer Credit

Students may receive a maximum of 9 graduate transfer credits toward a master's degree and 30 undergraduate transfer credits towards a bachelor's degree as evaluated using industry certifications. The limit for a total award of transfer credit, including both credits awarded for courses from other Universities and credit allocated from industry certifications, may not exceed 90 credit hours for a bachelor's degree and 18 credit hours for a master's degree. Three transfer credits may be used to meet credit requirements for the Graduate Certificates. Transfer 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 the receiving institution will accept credits or degrees earned at ECCU. An institution's licensure 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

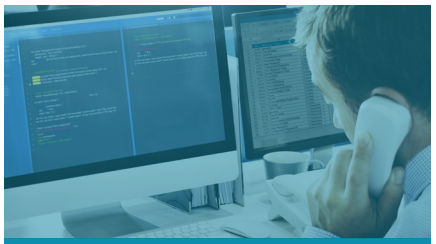
Graduate Programs

» Master of Science in Cyber Security

» Graduate Certificate Program

Graduate Certificate Program Selections:

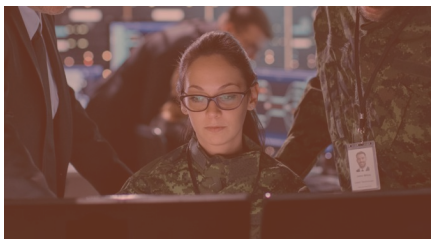
GRADUATE CERTIFICATE INFORMATION SECURITY PROFESSIONAL



GRADUATE CERTIFICATE SECURITY ANALYST

GRADUATE CERTIFICATE ENTERPRISE SECURITY ARCHITECT

GRADUATE CERTIFICATE INCIDENT MANAGEMENT & BUSINESS CONTINUITY



GRADUATE CERTIFICATE DIGITAL FORENSICS

GRADUATE CERTIFICATE EXECUTIVE LEADERSHIP IN INFORMATION ASSURANCE

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 cybersecurity applications, tools, and techniques used in today's job workforce for careers in cybersecurity. It prepares students to obtain knowledge for careers in information technology, and specifically in cybersecurity. The program features a state-of-the-art virtual lab environment to allow students hands-on experience in using the tools of a cybersecurity professional in a safe, secure online environment. It covers areas dealing with network management, computer security, incident response, and cybersecurity threat assessment; the program prepares the student for an entry-level position in the cybersecurity field.

BSCS 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. These program objectives are:

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

Bachelor's Degree Graduation Requirements

Each candidate for graduation must meet the following degree requirements:

- Completion of 60 credit hours of 300/400 level courses in which the candidate earned a cumulative GPA of 2.0 or better
- Completion of 120 + total semester credit hours including all transfer credit awarded
- Satisfactory completion (a grade of B- or higher) of the summative capstone course
- All degree requirements must be completed within one and a half times the program length as measured by maintaining a cumulative course completion rate of 67% of course work from the first term, the student enrolls in the University and begins the program to graduation.

BACHELOR OF SCIENCE IN CYBER SECURITY

Bachelor's degree courses

Core Courses: 30 Credits

CIS 300 – Fundamentals of Information Systems Security pg 26	3 Credits
CIS 301 – Legal Issues in Information Security pg 26	3 Credits
CIS 302 – Certified Threat Intelligence pg 26	3 Credits
CIS 303 – Security Policies and Implementation Issues pg 27	3 Credits
CIS 304 – Certified SOC Analyst pg 27	3 Credits
CIS 308 – Access Control, Authentication, and Public Key Infrastructure pg 27	3 Credits
CIS 403 – *Network Security, Firewalls, and VPNs (CND) pg 28	3 Credits
CIS 404 – *Hacker Techniques, Tools, and Incident Handling (CEH) pg 29	3 Credits
CIS 406 – *System Forensics, Investigation, and Response (CHFI) pg 30	3 Credits
CIS 410 – Capstone pg 31	3 Credits

Technical Electives: 15 Credits

Select 5 of the following courses:

CIS 401 – Security Strategies in Windows Platforms and Applications pg 28	3 Credits
CIS 402 – Security Strategies in Linux Platforms and Applications pg 28	3 Credits
CIS 405 – Internet Security: How to Defend Against Attackers on the Web pg 29	3 Credits
CIS 407 – Cyber Warfare pg 30	3 Credits
CIS 408 – Wireless and Mobile Device Security pg 30	3 Credits
CIS 409 – Fundamentals of Python pg 30	3 Credits

General Electives: 15 Credits

COM 340 – Communications and Technical Writing pg 32 (required)	3 Credits

Select 4 of the following courses:

BIS 430 – Ethics for the Business Professional pg 32	3 Credits
ECN 440 – Principles of Microeconomics pg 32	3 Credits
MGT 450 – Introduction to Project Management pg 33	3 Credits
MTH 350 – Introduction to Statistics pg 31	3 Credits
PSY 360 – Introduction to Social Psychology pg 31	3 Credits

*Certification exam available to take upon successful completion of the course

Total credit hours required for the BSCS Program	**60 Credits**

BACHELOR OF SCIENCE IN CYBER SECURITY

Grad Track Option

With EC-Council University's Grad Track option, a student can earn credits towards their Master of Science in Cyber Security program while completing their Bachelor of Science in Cyber Security degree. BSCS students can take a maximum of nine (9) credit hours of MSCS courses. These courses will be ECCU 500, ECCU 501, and ECCU 502, which will transfer to CIS 403, CIS 404, and CIS 406, respectively, into the BSCS program. These credits will count toward the BSCS program and can be applied to the MSCS degree if accepted into the program.

Eligibility Requirements

To qualify for a Grad Track option, you must:

- Be an active student at ECCU, pursuing a BSCS degree in their junior/senior year with at least 90 credit hours at the time of application to Grad Track;
- Have a 3.0 or higher cumulative GPA to begin a master's level course;
- Meet any prerequisite coursework requirements for each class; and
- Complete a Grade Track Form.

Benefits of the Grad Track Option

- BSCS/MSCS Career Advancement - reducing your MSCS program requirements from 36 credit hours to 27 credit hours = Completing your MSCS degree faster.
- Cost Saving - you get to pay the undergraduate rate for these three (ECCU 500, ECCU 501, and ECCU 502) Master's level courses (which will transfer to CIS 403, CIS 404, and CIS 406, respectively into the BSCS program).

Undergraduate level Courses

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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Discuss the field of ethics, describing how it differs from either law or religion, and why it is still necessary when we have both law and religion.

» Characterize three stances which can be applied to thinking about ethics: virtue ethics, utilitarianism, and deontological ethics.

» Explain ethical hacking, the hacker code and the particular problem of penetration testing.

» Examine ethical issues related to privacy.

» Identify surveillance practices.

» Discuss the problem of piracy and intellectual property theft.

» Discuss the specific ethics of cyberwarfare.

» Design techniques to protect given Windows networks and systems from security vulnerabilities.

» Explain what a Code of Ethics contains and what it means to practice professionalism in one's craft.

CIS 300 – Fundamentals of Information Systems Security (3 Credits)

It provides a comprehensive overview of the essential concepts readers must know as they pursue careers in cybersecurity systems. Part one opens with a discussion of the new cybersecurity 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 cybersecurity standards, education, professional certifications, and compliance laws.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Analyze the concepts of information systems security as applied to an IT infrastructure

» Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure

» Defend the role of access controls in implementing a security policy

» Explain the role of operations and administration in effectively implementing a security policy

» Prioritize the importance of security audits, testing, and monitoring to effective security policies

» Describe the principles of risk management, common response techniques, and issues related to the recovery of IT systems

» Explain how businesses apply cryptography in maintaining information security

» Analyze the importance of network principles and architecture to security operations

» Explain the means attackers use to compromise systems and networks and defenses used by organizations

» Apply international and domestic information security standards and compliance laws to real-world implementation in both the private and public sector

CIS 301 – Legal Issues in Cyber Security (3 Credits)

Addresses the area where law and cybersecurity concerns intersect. Cybersecurity 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 cybersecurity 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.

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Identify the legal aspects of information systems security (ISS)

» Examine the concept of privacy and its legal protections
» Distinguish the basic components of the American legal system
» Describe legal compliance laws addressing public and private institutions
» Analyze intellectual property laws
» Summarize cybercrime and tort law Issues in cyberspace

CIS 302 – Certified Threat Intelligence Analyst – C|TIA (3 Credits)

C|TIA is a method-driven course that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

The Purpose of C|TIA is: To enable individuals and organizations with the ability to prepare and run a threat intelligence program that allows 'evidence-based knowledge' and provides 'actionable advice' about 'existing and unknown threats.' To ensure that organizations have predictive capabilities rather than just proactive measures beyond active defense mechanism; to empower information security professionals with the skills to develop a professional, systematic, and repeatable real-life threat intelligence program; to differentiate threat intelligence professionals from other information security professionals. For individuals: To provide an invaluable ability to structured threat intelligence to enhance skills and boost their employability.

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Discuss various fundamental concepts about cyber threat intelligence, including its importance, types, lifecycle, strategy, capabilities, maturity model, frameworks, etc.

» Explain various stages of an attack and the deep dive scenario to build appropriate mitigation and defensive mechanisms to protect the organization from known and unknown threats

» Implement a threat intelligence program and identify the right team members to implement the program

» Communicate various concepts of threat intelligence data collection and processing, including its importance, types, feeds and sources, data collection management, storing and structuring of data, etc.

» Discuss various concepts of data analysis and threat analysis process along with techniques for fine-tuning threat analysis and the like, which helps the analysts to extract better threat intelligence

» Apply the techniques of evaluating the intelligence and creating a knowledge base for storing threat information

» Explain how to mitigate the risks posed by various cyber threats to improve the security posture of the organizations

CIS 303 – Security Policies and Implementation (3 Credits)

This course provides an overview of the security administration and fundamentals of designing security architectures. Topics include networking technologies, TCP/IP concepts, protocols, network traffic analysis, monitoring, and security best practices. Upon completion, students should be able to identify normal network traffic using network analysis tools and design basic security defenses. The course is designed to help prepare for the TestOut Security Pro certification exam.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Demonstrate methods for keeping networks and their computers secure

» Explain strategies for securing networks, including protection against viruses, worms, malware, and OS and application exploits

» Implement secure access through authentication and encryption

» Implement security policies

» Provide common application security, DNS, SMTP, HTTP, Instant Messaging, and other user and system accessible protocols with their implementation or protocol design weaknesses

» Ensure continuing security, detect active attacks through network traffic analysis, system and application log monitoring, and auditing. Track the warning signs of a problem or attack

» Discuss disaster planning and recovery issues such as redundancy, fault tolerance, power, and environmental conditioning, backups, recovery strategies, and clustering

» Troubleshoot security vulnerabilities. Demonstrate skills in penetration testing, by looking for and identifying weaknesses in configurations for operating systems, applications, firewalls, network devices, policies, and procedures in a given environment

CIS 304 – Certified Security Operations Center (SOC) Analyst (CSA)

This course will help the student to acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. It covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the student will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Prerequisites: CIS 300, CIS 301, CIS 302, and CIS 303.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Define basic concepts of SOC processes, procedures, technologies, and workflows

» Articulate concepts of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.

» Analyze logs and alerts from a variety of different technologies across multiple platforms

» Explain the architecture, implementation and fine-tuning of SIEM solutions and learn use cases that are widely used across the SIEM deployment

» Discuss the fundamental concepts on Threat Intelligence, different Threat Intelligence Platform (TIP), how it helps SOC and benefits of the integration of Threat Intelligence into SIEM

» Explain the Incident Response process and the importance of SOC and IRT collaboration for better incident response

CIS 308 – Access Control (3 Credits)

Access Control 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 cybersecurity 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.

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Define authorization and access to an IT infrastructure based on an access control policy framework

» Minimize risk to an IT infrastructure's confidentiality, integrity, and availability with sound access controls.

» Analyze how a data classification standard impacts an IT infrastructure's access control requirements and implementation

» Define proper security controls within the User Domain to mitigate risks and threats caused by human behavior

» Implement appropriate access controls for information systems within IT infrastructures

» Implement a secure remote access solution

CIS 401 – Security Strategies in Windows Platforms and Applications (3 Credits)

This course focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. The majority of individuals, students, educators, business 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 seven 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 step-by-step examples, this must-have resource will ensure its readers are educated on the latest Windows security.

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Explain the security features of the Microsoft Windows operating systems.

» Implement secure access controls when setting up Microsoft Windows in a given organization

» Configure encryption in a given organization to secure Windows environment

» Integrate controls to protect a given Windows system from malware

» Apply Group Policy controls and profile and audit tools to keep Windows systems secure

» Apply backup and restore operations on a given Windows system

» Apply best practices while managing changes to Windows and its applications

CIS 402 – Security Strategies in Linux Platforms and Applications (3 Credits)

Linux addresses the fundamentals of the Linux operating system. The course includes system architecture and history, system installation and configuration, the command line interface and shell commands, basic system administration, system updates, file systems, access controls, network services configuration, printer configuration, system services, security models, and scripting. The course is designed to help prepare for the TestOut Linux Pro certification exam.

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Discuss Linux operating system architecture, use cases, and general background

» Facilitate the Linux system installation and configuration

» Use command-line interfaces and shell commands

» Manage basic system administration and system updates

» Provide network services and printer configuration

» Manage Linux system services and security

» Complete the editing of files and scripting

» Create user accounts, user groups, user ownerships, and user permissions (access controls)

» Explain Linux cloud and virtualization

CIS 403 – Network Security, Firewalls, and VPNs (3 credits)

Provide a unique, in-depth look at the significant business challenges and cybersecurity 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. This book incorporates hands-on activities, using examples and exercises from the field to prepare the reader to disarm threats and prepare for emerging technologies and future attacks. Upon successful completion of this course, students may take the Certified Network Defender (CND) certification exam through EC-Council. If students wish additional information to assist them in preparing for the certification exam, they may purchase an iLab at an additional cost of $50.00.

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Discuss 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 security mechanisms, analyze available security controls and develop strategies to implement and configure these controls

» Explain the role of network security policies, and develop comprehensive policies that help in protecting network infrastructure

» Explain the working of various networking devices, and develop strategies for secure configuration of these devices

» Evaluate physical security mechanisms, examine the issues and recommend the countermeasures to safeguard the network infrastructure

CIS 404 – Hacker Techniques, Tools, and Incident Handling (3 Credits)

It begins with an examination of the landscape, key terms, and concepts that a cybersecurity 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.

Upon successful completion of this course, students may take the Certified Ethical Hacker (CEH) certification exam through EC-Council for a discounted price of $150. If students with additional information to assist them in preparing for the certification exam, they may purchase an iLab at an additional cost of $50.00

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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 the security of various components of the information system

» Compare and contrast different hacking techniques and analyze the legal implications of hacking

» Examine different 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 an appropriate level of information security controls based on evidence, information, and research

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 cybersecurity 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 secure web-enabled applications successfully.

Prerequisite: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Analyze the impact of the internet and Web applications on the business world

» Analyze the evolution of social media and social networking

» Examines the mobile device and connectivity security

» Compare and contrast Web-based risks

» Analyze common website attacks, weaknesses, and security best practices

» Describe the attributes and qualities of securing coding practices

» Analyze the role and importance of audit and compliance with Web application security

» Analyze the role and importance of quality assurance testing for Web applications

» Explain the value and importance of vulnerability and security assessments for web applications

» Evaluate next-generation challenges in securing web applications and data

» Construct a comprehensive lifecycle approach to Web application security

CIS 406 - System Forensics, Investigation, and Response (3 Credits)

This class is designed to provide the participants with the necessary skills to perform an effective digital forensics investigation. The course presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence. It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.

Upon successful completion of this course, students may take the Computer Hacking Forensic Investigator (CHFI) certification exam through EC-Council for a discounted price of $150.

Prerequisites: CIS 300, CIS 301, CIS 302 and CIS 303

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Discuss fundamental concepts of incident response and forensic, perform electronic evidence collection and digital forensic acquisition

» Explain web application forensics and its architecture, interpret the steps for web attacks, Apache web server architecture and its logs investigation

» Conduct thorough examinations of computer hard disk drives, and other electronic data storage media and recover information and electronic data from computer hard drives and other data storage devices

» Describe the strict data and evidence handling procedures, maintain an audit trail (i.e., chain of custody) and/or evidence of integrity, work on technical examination, analysis and reporting of computer-based evidence, preparing and maintaining case files

» Explain the use of mobile forensics, illustrate its architecture, mobile storage and its evidence

» Search file slack space where PC type technologies are employed, file MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences, examine file type and file header information, review e-mail communications; including web mail and Internet Instant Messaging programs, and examine the internet browsing history

CIS 407 – Cyber Warfare (3 Credits)

This course explores the cyberwarfare landscape, offensive and defensive cyber warfare techniques, and the future of cyber warfare. It also addresses military doctrine and strategies, intelligence operations, and cyberwarfare-related laws and ethics. Students will be exposed to many cybersecurity technologies, processes, and procedures that help to protect endpoints, networks, and data. They will also learn how to identify and analyze threat and vulnerabilities and create appropriate mitigation strategies

Prerequisites: CIS 300 and CIS 301

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Explain the importance of information as a military asset

» Describe the targets and combatants of cyber-warfare

» Explain the role of law and ethics in cyber-warfare

» Describe intelligence operations in cyber-warfare

» Describe cyberwarfare attackers and the evolution of cyber warfare techniques

» Summarize what cyber warfare may be like in the future

CIS 408 – Wireless and Mobile Device Security (3 Credits)

This course 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 the home. The growing use of mobile devices demands that organizations become more educated in securing this growing technology and determining how to protect their assets best-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.

Prerequisites: CIS 300 and CIS 301

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Deliver an overview of the evolution of wired, wireless, and mobile networks as well as their security risks

» Describe how WLANs work

» Outline WLAN and IP networking threat and vulnerability analysis

» Defend WLAN security measures

» Assess WLAN auditing and assessment

» Summarize mobile wireless attacks and remediation

CIS 409 – Fundamentals of Python (3 credits)

This course is an introduction to object-oriented design and data structures using the popular Python programming language. The level of instruction assumes at least one term/semester of programming in an object-oriented language such as Java, C++, or Python. Through the step-by-step instruction and exercises in this book, you'll cover such topics as the design of collection classes with polymorphism and inheritance, multiple implementations of collection interfaces, and the analysis of space/time tradeoffs of different collection implementations (specifically array-based implementations and link-based implementations). Collections covered include sets, lists, stacks, queues, trees, dictionaries, and graphs.

Course Learning Outcomes

Students who successfully complete this class will be able to**:**

» Discuss the basic structure of Python programs and know the different classes to represent new types of objects

» Define the four general categories of collections and know the difference between an abstract collection type and its implementations

» Determine the rate of growth of the work of an algorithm in terms of its problem size and how the sequential search and binary search algorithms work

» Explain how to develop an interface for a collection type and know the methods to manipulate bags and sets

» Use inheritance to share code among a set of classes and understand the methods of a set of classes into an abstract class

CIS 410 – Capstone Course (3 credits)

This course serves as a comprehensive assessment of knowledge and skills in information systems and cybersecurity. Activities include research into selected security problems and planning, designing, and implementing security solutions for a user organization.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Identify the objectives and detailed requirements of an Information Technology (IT) security services RFP

» Explain the procedures of a vendor bidder's conference

» Plan and perform a security compliance gap analysis

» Assess the effectiveness of existing security controls

» Conduct an enterprise-wide security assessment

» Prepare a qualitative risk and security assessment report

» Develop a plan to mitigate risks identified during the risk and security assessment

» Identify Business Impact Analysis (BIA), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) requirements that meet client's needs

» Design a layered security solution to protect IT assets

» Present a formal RFP response

COM 340 – Communications and Technical Writing (3 Credits)

This course is designed to prepare you in the basics of cybersecurity 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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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 a 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

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 the combined choices of their members. Economists study how people make decisions, how they work, what they buy, 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.

Course Learning Outcomes
Students who successfully complete this class will be able to**:**

» Explain concepts in trade

» Discuss the marketing forces of supply and demand

» Discuss government policies and their effect

» Explain taxation

» Discuss Competitive Markets and Monopolies

» Explain the Cost of Production

» Discuss Earnings, Poverty, and discrimination

» Discuss the Theory of Consumer Choice

COURSE DESCRIPTIONS

MGT 450 – Introduction to Project Mgmt. (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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Explain project characteristics through practice and implementation

» Determine the appropriateness of the project

» Define the requirements for scoping, scheduling, and costing a project using smart tools

» Manage identified project risks

» Communicate effectively with team and project stakeholders

» Measure the progress of a project

» Use digital tools to manage projects

» Assess the quality of the project, evaluate the factors involved in closing the project and demonstrate how legal standards affect the security strategy

MTH350 – Introduction to Statistics (3 Credits)

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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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.

» Conduct hypothesis tests.

» Think critically about information consumed in daily life and use an understanding of statistics to make the right decisions based on that information (statistical literacy).

PSY 360 – Social Psychology (3 Credits)

Why do individuals behave in a particular 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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Apply proper research techniques to produce comprehensive writings by utilizing course texts, readings, discussions, and presentations (Application, Critical Thinking, Communication)

» Discuss and critique topics in weekly group collaboration and activities to develop diverse and critical perspectives (Communication, Knowledge, Application)

» Identify and describe the terminology relevant to social psychology (Knowledge, Communication)

» 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

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 cybersecurity and assurance. The program consists of topical areas dealing with computer security management, incident response, and cybersecurity threat assessment, which require students to be creators of knowledge and inventors of cybersecurity processes, not merely users of information. Additionally, students will receive instruction in leadership and management in preparation for becoming cybersecurity 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:

» Application of cybersecurity technical strategies, tools, and techniques to secure data and information for a customer or client.

» Adherence to a high standard of cybersecurity ethical behavior.

» Use of research in both established venues and innovative applications to expand the body of knowledge in cybersecurity.

» Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the ever-changing environments of cybersecurity.

» Mastery of the skills necessary to move into cybersecurity leadership roles in companies, agencies, divisions, or departments.

Master's Degree Graduation Requirements

Each candidate for graduation must meet the following degree 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 (grade of B- or higher) of the summative capstone course;

» All degree requirements must be completed within one and a half times the program length as measured by maintaining a cumulative course completion rate of 67% of course work from the first term, the student enrolls in the University and begins the program to graduation.

MASTER OF SCIENCE IN CYBER SECURITY

Master of Science in Cyber Security Course Requirements

Core Requirements (27 Credits)

Core Research and Writing Skills Course

ECCU 505 – Intro to Research and Writing for the IT Practitioner pg 39 — 3 Credits

Core Management Emphasis Courses

ECCU 504 – Foundations of Organizational Behavior pg 39 — 3 Credits
ECCU 514 – Quantum Leadership pg 43 — 3 Credits
ECCU 516 – Hacker Mind: Profiling the IT Criminal pg 43 — 3 Credits
MGMT 502 – Business Essentials pg 38 — 3 Credits

Core Network Security Courses

ECCU 500 – *Managing Secure Network Systems (CND) pg 37 — 3 Credits
ECCU 501 – *Ethical Hacking and Countermeasures (CEH) pg 37 — 3 Credits
ECCU 507 – Linux Networking and Security pg 40 — 3 Credits

Final Requirement

ECCU 519 – Capstone pg 45 — 3 Credits

Pick one Specialization from below:

Specialization A: Security Analyst	Credits
ECCU 503 – *Security Analysis and Vulnerability Assessment (ECSA) pg 38	3
ECCU 506 – *Conducting Penetration and Security Tests (LPT-APT) pg 39	3
ECCU 509 – Securing Wireless Networks pg 40	3

Jobs

- » Information Security Manager/Specialist
- » Information Security Auditor
- » Risk/Vulnerability Analyst/Manager
- » Information Security Analyst
- » Penetration Tester
- » Security Architect
- » Computer Network Defender
- » Cybersecurity Defense Analyst
- » Information Security(IS) Director
- » Enterprise Architect
- » Security Architect
- » Research & Development Specialist
- » Systems Requirements Planner
- » System Testing and Evaluation Specialist
- » Information Systems Security Developer
- » Systems Developer
- » Technical Support Specialist
- » Network Operations Specialist
- » Cyber Defense Infrastructure Support Specialist
- » Vulnerability Assessment Analyst
- » Warning Analyst
- » Exploitation Analyst
- » All-Source Analyst
- » Mission Assessment Specialist
- » Target Developer
- » Target Network Analyst
- » All Source-Collection Requirements Manager
- » Cyber Intel Planner
- » Cyber Ops Planner
- » Partner Integration Planner
- » Cyber Operator
- » Chief Information Security Officer
- » Information Security Officer
- » Chief Security Officer
- » Information Assurance (IA) Program Manager
- » System Administrator
- » Multi-Disciplined Language Analyst
- » Information Assurance Security Officer

*Certification exam available to take upon successful completion of the course

MASTER OF SCIENCE IN CYBER SECURITY

Specialization B: Cloud Security Architect – Choose 3	Credits
ECCU 510 – Secure Programming pg 45	3
ECCU 520 – Advanced Network Defense pg 45	3
ECCU 524 – Designing and Implementing Cloud Security pg 44	3
ECCU 525 – Securing Cloud Platforms pg 47	3

Jobs

- » IT analyst
- » Systems analyst
- » Computer Network Architect
- » Enterprise Architect
- » Security Architect
- » Systems Requirements Planner
- » System Testing and Evaluation Specialist
- » Information Systems Security Developer
- » Systems Developer
- » Technical Support Specialist
- » Network Operations Specialist
- » System Administrator
- » Systems Security Analyst
- » Chief Information Security Officer
- » Information Security Officer
- » Chief Security Officer
- » Information Assurance Security Officer

Specialization C: Digital Forensics	Credits
ECCU 502 – *Investigating Network Intrusions and Computer Forensics (CHFI) pg 38	3
ECCU 517 – Cyber Law pg 44	3
ECCU 521 – Advanced Mobile Forensics and Security pg 46	3

Jobs

- » Forensic Analyst
- » Cyber Crime Investigator
- » Cyber Defense Forensics Analyst
- » Incident Responder
- » Chief Information Security Officer
- » Information Security Officer
- » Chief Security Officer
- » Information Assurance Security Officer

Specialization D: Incident Management and Business Continuity	Credits
ECCU 512 – Beyond Business Continuity: Managing Organizational Change pg 42	3
ECCU 513 – *Disaster Recovery (EDRP) pg 42	3
ECCU 522 – *Incident Handling and Response (ECIH) pg 46	3

Jobs

- » Director/Manager – Business Continuity
- » Information Assurance (IA) Program Manager
- » IT Project Manager
- » Director/Manager – Business Continuity
- » Cyber Defense Incident Responder
- » Incident Handler
- » Incident Manager
- » Incident Responder
- » Disaster Recovery Program Manager
- » Disaster Recovery Analyst
- » IT Disaster Recovery Analyst
- » Chief Information Security Officer
- » Information Security Officer
- » Chief Security Officer
- » Information Assurance Security Officer

Specialization E: Executive Leadership in Information Assurance	Credits
ECCU 511 – Global Business Leadership pg 41	3
ECCU 515 – Project Management in IT Security pg 43	3
ECCU 523 – *Executive Governance and Management (EISM/CCISO) pg 47	3

Jobs

- » IT Project Manager
- » Chief Information Security Officer
- » Information Security Officer
- » Chief Security Officer
- » Information Assurance Security Officer

+ Course has a proctored exam *Certification exam available to take upon successful completion of the course

Graduate Level Courses

ECCU 500 – Managing Secure Network Systems (3 credits)

This course focuses on evaluating network and Internet cybersecurity issues, designing, implementing successful security policies and firewall strategies, exposing the 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.

Upon successful completion of this course, students may take the Certified Network Defender (CND) certification exam through EC-Council.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Explain 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 cybersecurity 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 the 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.

Upon successful completion of this course, students may take the Certified Ethical Hacker (CEH) certification exam through EC-Council.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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 the security of various components of the information system

» Compare and contrast different cybersecurity hacking techniques and analyze the legal implications of hacking.

» Examine different cybersecurity 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 the appropriate level of information 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.

Upon successful completion of this course, students may take the Computer Hacking Forensic Investigator (CHFI) certification exam through EC-Council.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Discuss fundamental concepts of incident response and forensic, perform electronic evidence collection and digital forensic acquisition

» Explain web application forensics and its architecture, interpret the steps for web attacks, Apache web server architecture and its logs investigation

» Conduct thorough examinations of computer hard disk drives, and other electronic data storage media and recover information and electronic data from computer hard drives and other data storage devices

» Explain the strict data and evidence handling procedures, maintain an audit trail (i.e., chain of custody) and/or evidence of integrity, work on technical examination, analysis and reporting of computer-based evidence, preparing and maintaining case files

» Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images, and other files, gather volatile and non-volatile information from Windows, MAC, and Linux, and recover deleted files and partitions in Windows, Mac OS X, and Linux

» Discuss network forensics and its steps involved, examine the network traffic, understand the email terminology and its characteristics, review the steps for investigating the email crimes

» Explain the planning, coordination and direct recovery activities and incident analysis tasks, the examination of all available information and supporting evidence or artifacts related to an incident or event

» Conduct data collection using forensic technology methods in accordance with evidence handling procedures, including a collection of hard copy and electronic documents, conduct reverse engineering for known and suspected malware files, and Identify of data, images and/or activity which may be the target of an internal investigation

» Explain the mobile forensics and illustrate its architecture, mobile storage and its evidence

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 cybersecurity 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.

Upon successful completion of this course, students may take the EC-Council Certified Security Analyst (ECSA) certification exam through EC- Council.

Prerequisite: ECCU 501

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Monitor, capture, and analyze network traffic and identify the possible cybersecurity breaches.

» Identify the various computer security issues and select a 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 primary facets of organizational theory and defining requisite skills. This course walks the cybersecurity practitioner through who he/she is as an individual worker and how they fit into an organizational process, defines the 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 see how the character's behaviors impinge upon the structure in a variety of ways.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Provide an overview of organizational behavior, and discuss the nature and impact of changing the environment of organizations

» Discuss the foundations of individual behavior and characterize the motivation in organizations

» Relate motivation and employee performance, and identify the key elements in motivating employee performance through work and rewards

» Identify and describe common causes of stress, and various ways of managing stress and the work-life balance

» Describe and distinguish the nature of decision making and problem-solving, and discuss the foundations of interpersonal and group behavior

» Identify and discuss the types and benefits of using teams, and describe the needs, modes, and benefits of communication in organizations

» Discuss traditional models for understanding leadership and contemporary views of leadership in an organization

» Define and discuss the influence of power, politics, and organizational justice, and describe ways to manage conflict and negotiation in the organization

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.

Course Learning Outcomes
Students who successfully complete this class will be able to:
» 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

» Finding the thesis statement

» 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 the 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.

Upon successful completion of this course, students may take the Licensed Penetration Tester (LPT) certification exam through EC-Council.

Prerequisite: ECCU 503

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Examine various penetration testing mechanisms and choose a suitable set of tests that balance cost and benefits

» Apply the penetration testing techniques and perform the intensive assessments of an organization's infrastructure to effectively identify risks

» Demonstrate the compliance of the cybersecurity 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 cybersecurity measures in protecting information resources from attack

» Perform internal and external penetration test audits on network infrastructure components and analyze the results

» 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 explores the various tools and techniques commonly used by Linux system administrators. It is designed for students who have limited or no previous exposure to Linus. Emphasis is placed on writing a simple bash script, using a text editor, manage processes within the Linux file system. Additional topics include making data secure, user security, and file security. 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

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Effectively use research to understand the fundamentals of a Linux platform and analyze the file system

» Analyze different 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 frame policies, guidelines and best practices for information security in the organization

» Discuss 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 an appropriate level of 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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Discuss the fundamental concepts of wireless network and wireless network security

» Discuss the terminologies, explore the technology trends for next-generation wireless networks, and examine the functioning of various wireless devices connected to the network

» Explain how the performance of wireless networks depends on factors such as the protocols used and assess the role of communication standards in the 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)

Certified Application Security Engineer (CASE) is a hands-on, Instructor-led, comprehensive application security course, which encompasses security activities involved in all of the phases of the Software Development Lifecycle (SDLC). The course also focuses on selecting and implementing the right security strategies, guidelines, and practices that are widely accepted and applicable to most environments used today.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Implement a standard set of secure programming practices, policies, and guidelines to develop robust sofware applications.

» Compare various application development models and methodologies and implement a threat modeling 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.

» Discuss 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 a shared vision, maintaining a competitive advantage, integrity, and leading for change.
This is a study of current and historical leadership theories with an emphasis on viewing the leadership function in the context of global organizational behavior and organizational designs.

Prerequisite: ECCU, 505.

Course Learning Outcomes

Students who successfully complete this class will be able to:

» 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 cybersecurity 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

Course Learning Outcomes

Students who successfully complete this class will be able to:

» 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

» Communicate 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 reach 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 cybersecurity 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.

Upon successful completion of this course, students may take the EC-Council Disaster Recovery Professional (EDRP) certification exam through EC-Council.

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Explain the various types of disasters and analyze their consequences and effects on an organization.

» Evaluate the need for cybersecurity disaster recovery and identify the phases involved in the process of recovery.

» Prepare and implement a 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, the role of certification and accreditation authority in securing information systems and identify the technology or services required to recover the data.

» Discuss 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.

» Explain 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 for understanding the process of leadership. The study describes the roles, functions, and impact of global leadership concepts. Numerous team exercises facilitate the speed at which leadership must adapt to be current. Research and views into how most cultures respond to this area of management are provided as well as compared and discussed.

Prerequisite: ECCU 505

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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 vital 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 a cybersecurity planning perspective - specifically IT Project Management. Students will learn how to use the 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.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Illustrate the factors that influence the success of the project and define and explain how to create an 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 cybersecurity 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 a cybersecurity 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)

Cyberspace 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 international terrorists. The IT criminal threatens businesses, governmental agencies, militaries, and organizations of every kind. This course will survey the full spectrum of psychological attributes that constitute the profile of the IT criminal.

Prerequisite: ECCU 505

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Apply proper research techniques to produce comprehensive writing by utilizing course texts, reading, 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, 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 cybersecurity 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 cybercrimes upon the traditional notions of sovereignty and current events that affect cyber laws.

Prerequisite: ECCU 505

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet cybersecurity.

» Discuss different types of cybercrimes and analyze legal frameworks of different countries to deal with these cybercrimes.

» Describe the importance of jurisdictional boundaries and identify the measures to overcome cross-jurisdictional cyber crimes.

» Describe the importance of ethics in the legal profession and determine the appropriate ethical and legal behavior according to legal frameworks.

» Identify intellectual property rights issues in 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 cybersecurity 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 (3 credits)

Special topics courses will be offered from time to time as a substitution for another course. This course will be considered as an elective.

Prerequisites: ECCU 500 and 505

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 successful completion of all core degree requirements but must be within six credit hours of graduation. Students must demonstrate attainment of a 3.0 cumulative grade point average and have the Registrar approval to register in this class.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Conduct cybersecurity needs assessments, analyze the internal and external cybersecurity threats, and determine and implement the

methodologies to secure the cybersecurity systems of an organization.

» Conduct a cybersecurity audit of a complete information system

» Identify a cybersecurity attack, collect necessary evidence in a forensically sound manner, and trace the perpetrator of a crime.

» Implementthebest 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 cybersecurity 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 appropriate personnel that is impacted by the cyber-attack by designing and implementing standard cybersecurity policies, procedures, and pieces of training.

» Identify the common thread to the organizational impact as well as the security impact of continuous network innovations.

» Define a set of useful ideas or "laws of identity" that an IS technician can use to reduce insider threat.

ECCU 520 – Advanced Network Defense (3 credits)

This course focuses on the fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and how to harden your enterprise architecture from the most advanced attacks. It provides segmentation and isolation to reduce the effectiveness of advanced persistent threats.

Prerequisite: ECCU 501

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Explain how to expose weaknesses for system's owners to fix breaches before being targets of compromise.

» Demonstrate expertise in identifying security weaknesses in computer systems or networks.

» Apply necessary techniques required for malware identifi¬cation throughout the enterprise even in the case of the malware not being detectable by any of your security controls.

» Discuss and analyze best practices in developing a secure system and network configurations.

» Explain how to establish a secure baseline in deploying machines in a protected state and demonstrate popular attack methods applied by hackers to fortify their systems.

» Learn how to execute a set of techniques that are critical to the detection and prevention of various threats and intruding activities.

» Apply pen testing, hacking constructively to analyze, defend against various possible attacks, and protect your entire enterprise against some of today's most advanced threats.

» Discuss how to stage advanced attacks to appreciate methods of correctly eliminating or mitigating risk to an acceptable level.

ECCU 521 – Advanced Mobile Forensics and Security (3 credits)

This course focuses on the intricacies of manual acquisition (physical vs. logical) and advanced analysis using reverse engineering to understand how popular Mobile OSs are hardened to defend against frequent attacks and exploits. Topics include mobile forensic challenges and process, mobile hardware design and architectures, OS architecture, boot process, and file systems, threats and security, evidence acquisition and analysis, application reverse engineering, and mobile forensics reporting and expert testimony.

Prerequisites: ECCU 501 and ECCU 502

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Outline the frequent attacks through Mobile Device Security Hardening and understand what works best for corporate users.

» Explain how to refine current mobile forensic processes by addressing its unique problems of preserving crucial data and producing valid results.

» Describe how a Digital or Mobile Forensic Investigator processes cell phones, PDAs, and any other mobile devices that can store data and communicate.

» Explain how to protect your organization by retrieving stolen data and incriminating evidence from communications devices used by rogue employees and by conducting proper & regular IT Audit investigations on mobile devices to ensure no misuse of company information.

» Discuss various elements of Mobile Device Hacking such as the latest genre of attacks from simple password cracking to sophisticated injection of rootkits / remote spy monitoring and identify various mobile threat agents.

» Compare and contrast various Mobile forensics and analysis Tools

» Comprehend the concepts of Mobile Reverse Engineering and Outline the skills required for performing it.

» Discuss how to influence results of civil, private litigation and criminal cases by providing crucial evidence such as the suspects involved, their locations at the time of questioning, and the role they played by extracting this information from mobile devices.

» Investigate the processes involved in Mobile Forensic Acquisitions, Analysis and Reporting of Mobile Device evidence with detailed coverage on some of the popular devices.

ECCU 522 – Incident Handling and Response (3 credits)

This course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Additional emphasis is placed on computer forensics and its role in handling and responding to incidents. Through this course, students will be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, insider attack threats, incident response teams, incident management training methods, and incident recovery techniques in detail.

Prerequisite: ECCU 501
Upon successful completion of this course, students may take the EC-Council Certified Incident Handler (ECIH) certification exam

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Demonstrate fundamental skills that are required to handle and respond to computer security incidents in an information system.

» Discuss various types of incidents, risk assessment methodologies, and check for precautions.

» Discuss various principles, processes, and techniques for detecting and responding to security threats/breaches.

» Demonstrate how to handle incidents, conduct assessments, and comprehend various incidents like malicious code, network attacks, and insider attacks.

» Explain the role of computer forensics in handling and responding to the incidents.

» Discuss incident response teams, incident reporting methods, and incident recovery techniques.

» Explain various laws and policies related to incident handling and learn how to liaison with statutory and regulatory bodies.

ECCU 523 – Executive Governance Management (3 credits)

This course is designed to bring together all the components required for a C-Level position by combining Governance, Security Risk Management, Controls, and Audit Management, Security Program Management and Operations, Information Security Core Concepts, Strategic Planning, Finance, and Vendor Management, to lead a highly successful IS program.

Upon successful completion of this course, students may take the EC-Council Information Security Manager (EISM) or Certified Chief

Information Security Officer (CCISO) certification exam.

Prerequisite: ECCU 501

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Define, implement, manage, and maintain an information security governance program that includes leadership, organizational structures, and processes.

» Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards, and policies.

» Analyze all the external laws, regulations, standards, best practices applicable to the organization, and understand the federal and organization-specific published documents to manage operations in a computing environment.

» Produce information systems control status reports to ensure that the processes for information systems operations, maintenance, support meet the organization's strategies and objectives, and thereby share with relevant stakeholders to support executive decision-making.

» Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting an organization's objectives

» Evaluate the project management practices and controls to determine whether business requirements are achieved costs effectively while managing risks to the organization.

» Identify the criteria for mandatory and discretionary access control, understand the different factors that help in the implementation of access controls, and design an access control plan.

» Explain various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks.

» Develop, implement, and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives.

» Explain the acquisition lifecycle and determine the importance of procurement by performing Business Impact Analysis.

ECCU 524 – Designing and Implementing Cloud Security (3 credits)

This course focuses on and provides comprehensive knowledge of cloud services, their characteristics, benefits, applications, and service models. It covers planning, designing, and implementing cloud security controls. It delves into various cloud standards, countermeasures, and best practices to secure information in the cloud. The program also emphasizes the business aspects of cloud security, such as cloud uptime, uptime guarantee, availability, fault tolerance, failover policy, and how cloud security strengthens the business case for cloud adoption.

Prerequisite: ECCU 501

Course Learning Outcomes

Students who successfully complete this class will be able to:

» Discuss the fundamentals of cloud computing, cloud services, cloud computing service models, deployment models, and security considerations of cloud computing.

» Explain secure cloud computing environment design

» Explain cloud computing standards, Outline impacts of cloud outage/ failure, and discuss best practices for optimal cloud performance.

» Discuss best practices of virtualization and cloud implementation.

» Discuss various types of attacks on a cloud environment and techniques to overcome attacks.

» Explain various configuration management techniques, risk assessment methodologies, penetration testing, and Intrusion detection systems (IDS) for a secured cloud environment.

» Differentiate the compliance to established industry standards, acts, and laws including PCI-DSS, HIPAA, Sarbanes-Oxley, and Data Protection Act.

» Discuss the legal issues such as cloud computing contracts, vendor transitioning, auditing cloud data, maintaining privacy and confidentiality, geographic jurisdiction, limitations on vendor liability, and taxation challenges.

» Discuss Mobile Cloud Computing (MCC) and discuss best practices for secured mobile cloud access.

» Discuss best practices of virtualization and cloud implementation.

ECCU 525 – Securing Cloud Platforms (3 credits)

The sole purpose of this course is to reduce operating costs and increase efficiency by getting rid of on-premise servers; however, poor cloud security practices defeats this purpose as your environment might be open to attacks like ransomware, denial of service, data breach, and other activities that might cause irreversible damage to your company revenue and reputation or even completely shut down the business.

This course will guide you on how to best manage the risk in your cloud environment with good overall security practices ranging from user accounts, data, and network. We will also focus on the largest cloud computing providers.

Prerequisite: ECCU 501

Course Learning Outcomes
Students who successfully complete this class will be able to:

» Select the right cloud service solution in terms of security and protecting data at rest on AWS.

» Review audit logs to see security events on AWS accounts.

» Explain Azure RBAC and how to leverage it to protect your environment.

» Manage a network security group and apply different security policies depending on security requirements, be it internal, external, or your DMZ network.

» Explain the concept of application control and integrity monitoring, and know how to reach from unexpected changes, possibly malicious, on your Azure environment.

» Explain how to use Salesforce authentication and user management and learn how to set up an audit trail on the Salesforce cloud environment.

» Use Oracle Cloud IAM and understand how to use Oracle vaults for centralized storage of keys, database, and audits.

» Differentiate authentication methods and apply the best-suited authentication techniques for your environment. configure server-level IP firewall rules to control network traffic to your database.

» Discuss Google Infrastructure and its implemented security layers.

» Use Cloud Security Scanner, Apigee, Binary Authorization, and Vulnerability scanner to secure your application on the cloud.

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 Cybersecurity fields. It covers the latest changes in Information Technology for Business, also including computer-aided manufacturing (CAM), application software, and recent ethical issues arising from IT. Real-life business examples are added throughout the course that reinforces the business principles.

Course Learning Outcomes
Students who successfully complete this class will be able to:

» 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 conventional legal and political issues among nations that affect 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.

» Discuss the impact of Information Technology on the business world, and identify the threats and risks IT cybersecurity poses for businesses.

» Discuss some of the institutions and activities in international banking structures and global finance.

GRADUATE CERTIFICATE PROGRAM

This is a graduate-level academic program offering specialty areas of study in the cybersecurity field.

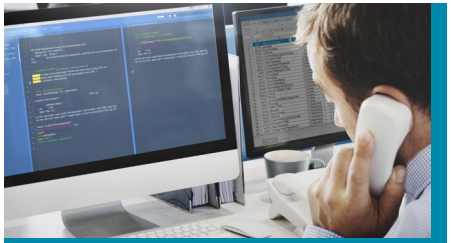
The EC-Council University Graduate Certificate Program provides the opportunity for students to earn graduate-level credit in specialty areas of study in the cybersecurity field. The program is targeted towards students wanting to advance in their careers or change their job focus. The courses offered through the graduate certificate program allows students to sharpen and learn new skills and deepen their knowledge within a specialty area. The certificates can be added to a student's professional portfolio and used for career change or advancement. The courses offered through the Graduate Certificate Program are the same courses required for the Master's degree, simply bundled in highly focused groupings.

There are six EC-Council University Graduate Certificates: Information Security Professional, Security Analyst, Enterprise Security Architect, Digital Forensics, Incident Management, and Business Continuity, and Executive Leadership in Cyber Security. Please see the specific course requirements for each certificate listed in the catalog.

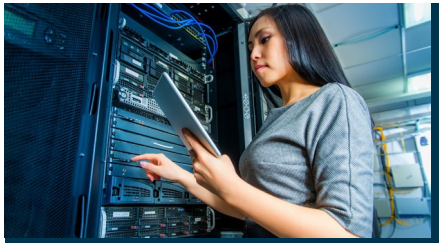
The Graduate Certificate Program does not lead to industry certifications.

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. Graduate Certificate courses can be applied to the MSCS degree.

GRADUATE CERTIFICATE INFORMATION SECURITY PROFESSIONAL

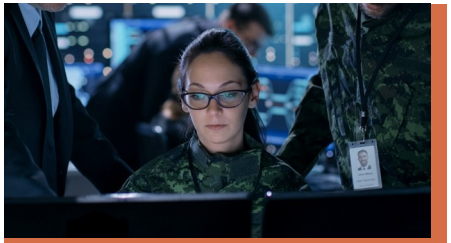


GRADUATE CERTIFICATE SECURITY ANALYST



GRADUATE CERTIFICATE ENTERPRISE SECURITY ARCHITECT

GRADUATE CERTIFICATE INCIDENT MANAGEMENT & BUSINESS CONTINUITY



GRADUATE CERTIFICATE DIGITAL FORENSICS

GRADUATE CERTIFICATE EXECUTIVE LEADERSHIP IN INFORMATION ASSURANCE

GRADUATE CERTIFICATE PROGRAM

I. ECCU Graduate Certificate – Information Security Professional

Required Courses:

ECCU 500 Managing Secure Network Systems (CND)	3 Credits
ECCU 501 Ethical Hacking and Countermeasures (CEH)	3 Credits
ECCU 505 Research and Writing for the IT Practitioner	3 Credits

Total credit hours **9 Credits**

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

II. ECCU Graduate Certificate – Security Analyst

Required Courses:

ECCU 503 Security analyst and Vulnerability Assessment (prerequisite ECCU 501 (CEH)) (ECSA)	3 Credits
ECCU 506 Conducting Penetration and Security Tests (prerequisite ECCU 501-CEH and ECCU 503 (ECSA)) (LPT)	3 Credits
ECCU 509 Securing Wireless Networks	3 Credits

Total credit hours **12 Credits**

ECCU Graduate Certificate – Security Analyst focuses on testing methods and techniques to effectively identify and mitigate risks to the security of a company's infrastructure, while providing application and network-based security vulnerability assessments, penetration tests, securing wireless networks including authentication, authorization, and encryption in accordance with industry-accepted methods and protocols.

III. ECCU Graduate Certificate - Enterprise Security Architect

Courses: (Choose 3)

ECCU 510 – Secure Programming	3 Credits
ECCU 520 – Advanced Network Defense (prerequisite ECCU 501-CEH)	3 Credits
ECCU 524 – Designing and Implementing Cloud Security (prerequisite ECCU 501-CEH)	3 Credits
ECCU 525 – Securing Cloud Platforms (prerequisite ECCU 501-CEH)	

Total credit hours **15 Credits**

ECCU Graduate Certificate – The Enterprise Security Architect specialization focuses on planning, analyzing, designing, configuring, testing, implementing, maintaining, and supporting an organization's on-premise and cloud security infrastructure.
The Cloud Security Architect Graduate Certificate trains you to harden enterprise architecture and cloud architecture from the most advanced attacks and secure programming practices to overcome these inherent drawbacks to pre-empt bugs from the code, and designing and implementing course security.

IV. ECCU Graduate Certificate – Digital Forensics*

Required Courses:

ECCU 502 Investigating Network Intrusions and Computer Forensics (CHFI)	3 Credits
ECCU 517 Cyber Law (prerequisite ECCU 505)	3 Credits
ECCU 521 Advanced Mobile Forensics and Security (prerequisite ECCU 501-CEH)	3 Credits

Total credit hours **15 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.

V. ECCU Graduate Certificate – Incident Management and Business Continuity

Required Courses:

ECCU 512 Beyond Business Continuity (prerequisite ECCU 505)	3 Credits
ECCU 513 Disaster Recovery - (EDRP)	3 Credits
ECCU 522 Incident Handling and Response (ECIH) (prerequisite ECCU 501-CEH))	3 Credits

Total credit hours **12 Credits**

EECCU Graduate Certificate – Incident Management and Business Continuity focuses on handling and responding to various security incidents, identifying vulnerabilities and taking appropriate countermeasures to prevent information failure risks, and 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.

VI. ECCU Graduate Certificate – Executive Leadership in Information Assurance

Required Courses:

ECCU 511 Global Business Leadership (prerequisite ECCU 505)	3 Credits
ECCU 515 Project Management	3 Credits
ECCU 523 Executive Governance and Management (EISM/CCISO) (prerequisite ECCU 501-CEH)	3 Credits

Total credit hours **15 Credits**

ECCU Graduate Certificate – The Executive Leadership in Information Assurance is designed to train Chief Information Security Officers, the skill set required to lead an efficient and

TESTING FOR EC-COUNCIL CERTIFICATIONS

Many of the core courses in the Master's and Bachelor's degree program parallel the knowledge requirements for EC-Council certifications.

Once a student has completed and passed the corresponding ECCU course, then they are eligible to test for the EC-Council certification. Students must pass the test to achieve the certification.

Receiving a passing grade in the ECCU course does NOT guarantee a student will pass the certification exam. Students are responsible for the cost of the LPT Advanced and CCISO exams.

To take the exam, students must contact EC-Council University to complete an exam voucher. If the certification exam is NOT passed the first time, ECCU students may purchase additional vouchers at the student rate of $150. For more information, contact ECCU at registrar@eccu.edu.

Certification	Masters Course	Bachelors Course
Certified Network Defender (CND)	ECCU 500 Managing Secure Network Systems	CIS 403 Network Security, Firewalls, and VPNs
Certified Ethical Hacker (CEH)	ECCU 501 Ethical Hacking & Countermeasures	CIS 404 Hacker Techniques, Tools, and Incident Handling
Computer Hacking Forensic Investigator (CHFI)	ECCU 502 Investigating Network Intrusions and Computer Forensics	CIS 406 System Forensics, Investigation, and Response
EC-Council Certified Security Analyst (ECSA)	ECCU 503 Security Analysis and Vulnerability Assessment	
Licensed Penetration Tester (LPT) (Master)	ECCU 506 Conducting Penetration and Security Tests	
EC-Council Disaster Recovery Professional (EDRP)	ECCU 513 Disaster Recovery	
EC-Council Certified Incident Handler (ECIH)	ECCU 522 Incident Handling and Response	
EC-Council Information Security Manager (EISM)	ECCU 523 Executive Governance and Management	
Certified Chief Information Security Officer (CCISO)	ECCU 523 Executive Governance and Management	

INTERNSHIPS AND CAPSTONE PROJECTS

Earn Real Life Experience

Learn valuable new skills outside of a traditional classroom. While exploring your career interests, you will be able to acquire knowledge of the field, industry, and employer simultaneously.

Develop New Skills

Build your soft, non-technical skills as well as your hard, technical skills. Employers seek new job candidates who can mix soft skills, such as communication and leadership, with hard- skills that are associated with the specific skill set required in a job.

Gain Competitive Advantage

Internship experience can provide you with an advantage when you apply for jobs upon graduation by adding work experience to your credentials.

Internships are a form of professional learning experience that integrates practical knowledge and learned classroom skills that will allow students to build and develop career paths, gain practical work experience, build their resume, and grow professional connections in their career field.

Students at ECCU have a choice to pick a Capstone project or an Internship program in their Capstone course. The capstone project can allow a working adult to apply technical knowledge gained from the program to work-related projects as applied learning. The Internship can serve as an alternative for a Capstone project. Students participating in a for-credit internship must be registered for a related course, are required to complete graded assignments in relation to their work with organizations, and are advised by faculty during their work term. Students enrolled in a for-credit internship course are expected to intern a minimum of 12 hours per week during the 12-week term. Full-time internships students are required to work 20-35 hours or more per week. Program internships can be paid or unpaid. The internship is considered as 3-credit or 135 contact hours.

INTERNSHIPS AND CAPSTONE PROJECTS

Why Intern

ECCU team will assist in matching students based on their learning experience, skills, and academic specializations. ECCU will help provide students with ongoing support in all aspects of the internship experience. All internship jobs are pre-qualified to meet ECCU standards and guidelines established for internships by the Department of Labor Fair Labor Standard Act and adherence to ECCU International Internship Policies. Through this internship program, student benefits the following outcomes:

Learn on the Go

Gain in-depth industry knowledge and experiences, develop industry-specific skills and skills necessary for future opportunities. Gain the opportunity to attain a valuable applied experience that is consistent with your career path while developing teamwork, communication skills, decision-making skills, and social responsibility.

Increase Your Job Opportunities

Broaden your chance of landing a job and jump-starting your career by building your resume.

Network with the Experts

Grows your connections and professional network in the right industry by meeting professional role models and potential mentors who can provide guidance, feedback, and support.

INTERNSHIPS AND CAPSTONE PROJECTS

Eligibility Criteria

To be eligible for the Internship Program, ECCU students need to adhere to the following:

» Students must be registered as a full-time student at the University with 90 earned undergraduate credits or 30 graduate credits, have a cumulative grade point of at least 2.0 undergraduate and 3.0 for graduate students, and have the approval of their academic dean.

» Students participating in a for-credit internship must be registered for a related course, are required to complete graded assignments in relation to their work with organizations, and are advised by faculty during their work term. Students enrolled in a for-credit internship course are expected to intern a minimum of 12 hours per week during the 12-week term. Full-time internships students are required to work 20-35 hours or more per week.

Intern Reporting Requirements

The success of an internship depends on the partnership between representatives of the organization, the university, and the student. These parties need to agree on the conditions of the internship, the responsibilities of each party, and the reporting requirements. Part of reporting requirements for interns are:

Identified Learning Goals

The learning contract allows the intern to document how, when, how often, with whom, etc., the learning goals are accomplished. The learning contract is a tool to formalize the internship. It includes information such as a description of the internship responsibilities (job description), goals and objectives, and how objectives will be met and assessed.

Identified learning goals allow students to assess their progress, as well as allowing the internship mentor/supervisor to be able to assess the students. The mentor/supervisor, the intern, and the academic dean will sign the learning contract. Each partner will have a clear understanding of the expectations of the experience and what the final results should be.

Academic Assignments

This monitoring mode encourages reflection about the learning experience and invites the intern to reflect on the experience critically and to evaluate each learning goal outlined in the internship objectives. This method encourages interns to evaluate their experience in a more analytical manner, especially in relation to the context of other life experiences, their curriculum, and major field of study.

INTERNSHIPS AND CAPSTONE PROJECTS

Mid Term Check-In

The mentor/supervisor, the intern, and the academic dean will closely monitor the progress of the internship through written reports of job tasks learned, site visits, phone calls, and evaluations.

Final Evaluations

To be completed by both the intern and mentor/supervisor as a way to identify critical areas of

success. Identify areas for improvement for the intern and the internship site.

Highlight personal strengths and prescribe solutions for the intern's professional development.

Learning / Job Connections

Internships and capstone projects allow for applied avenues of academic knowledge in real-world / workplace settings. This facilitates a student being armed with work experience that, combined with academic degrees and industrial certifications, gives a student a broader tool kit of credentials to gain career advancement. These types of applied academic learning experiences combined with ECCU's Cybersecurity Advancement Alliance program that promotes collaboration between the university and the cybersecurity industry provides improved opportunities to align learning outcomes with the needs of industry in hiring and placement. Often internship placements lead to fulltime job opportunities at the company of internship as the university, knowledge, student, and the company is all known to each other.

Applying for Internships

Students would seek internship opportunities in their local area through the networking activities of the university, corporate partners, and student initiative. Various online job service sites serve the internship market and work placements in similar ways to job search.

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 three courses per term. Students that are taking fewer courses a term will be considered part-time. All degree requirements must be completed within one and a half times the program length as measured by course completion rate of 67% of course work from the first term the student enrolls in the University and begins the program to graduation.

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.

STUDENT SERVICES

Credits

All credits awarded by EC-Council University are semester hour credits and equate with the formula of 45 hours of student work per credit hour per term (15 hours of engagement and 30 hours of preparation). A 3-credit hour course would have 135 of work, 45 hours of engagement, and 90 hours of preparation. This would equate to approximately 11 hours of work per week of the term per course.

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

To be considered full-time, MSCS students must take 6-semester hour credits per term, and BSCS students must take 9-semester hour credits per term. Three-quarter time is two courses per term (6 semester hour credits) for bachelor students. There is no three-quarter time for Master's students. Half time is considered one course per term for Master's students (3 semester hour credits).

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 11.25 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 12. The Dean must approve additional credit hours.

Minimum Academic Achievement

Graduate degree candidates must maintain a cumulative GPA of 3.0 or higher. Undergraduate degree candidates must maintain a cumulative GPA of 2.0 or higher. Failure to maintain this GPA will result in students being placed on academic probation or suspension. See the below section entitled Satisfactory Academic Progress for more details.

Maximum Program Length

A student must complete the entire program within one-and-one-half times the program length as measured by a successful completion rate of 67% of courses attempted.

Attendance and Participation

Students are expected to participate weekly in all class sessions and assigned activities. Extenuating circumstances that 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.

Failure to participate in a given week's work will result in the student being placed on Attendance Probation, and they will have one week to show participation. A failure to participate during Attendance Probation will result in the student being placed on Attendance Suspension, and they will have one week to show participation. A failure to participate during Attendance Suspension will result in course withdrawal retroactive to the last date of recorded attendance.

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.

Satisfactory Academic Progress

A student must continuously maintain Satisfactory Academic Progress (SAP) toward completion of their degree program to remain in good academic standing, regardless of their course load.

The University GPA is the official GPA on the student transcript. It is a cumulative GPA for the student's current program (undergraduate or graduate). Grades of I and W are not included in the GPA calculation. SAP is recalculated for changes to GPA after I grades have been updated to a letter grade. Incomplete (I) is changed to an F if not completed within 21 days from the end of the course.

If you retake a course, your GPA for SAP purposes will be calculated based on the highest grade received for the course. However, when calculating your Percentage of Credit Completion, both courses will count towards the 150% of their program length to complete their degree before they become ineligible to receive financial aid (including federal Direct and Plus loans).

SAP is evaluated at the end of every term, regardless if the student receives financial aid for the term. At the end of the first term, the first violation results in the student being placed in SAP Warning. At the end of the second term, the second violation results in the student moved to SAP Suspension and the potential loss of financial aid eligibility. Students will be allowed to appeal and be placed on SAP Probation. After three terms not

meeting SAP a student will be suspended from financial aid as well as the University. Students currently receiving financial aid will receive notification of their warning or violation status, to their official university email address, when they are below their required GPA, or get close to meeting their completion date and/or maximum timeframe.

If an undergraduate student has 60 or more non-passing credit hours a review will also be done to determine if they can complete their program within the maximum timeframe. If it is determined that a student cannot complete their program within the maximum timeframe, they will be automatically suspended from receiving financial aid without a warning letter.

Transfer credits are not considered in the calculation of the student's ECCU cumulative GPA. Transfer credits accepted will count for both attempted and completed credits for the SAP calculation of pace of completion (Percentage of Credit Completion - PCC).

SAP is defined as a 3.0 cumulative GPA for Master's and Graduate Certificate and a 2.0 cumulative GPA for Bachelor's 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 Registrar and be placed on Academic Probation (AP). The notice will identify the requirements to be met by the student in order to be removed from Academic Probation. A copy of the notice will become part of the student's permanent file.

Criteria for maintaining continual SAP

Students are expected to remain actively engaged in their academic work, including weekly participation in discussions and handing in assignments. They are expected to maintain the following minimum grade point averages and percentage of credit completion.

» Bachelor's level students are required to maintain a CGPA of 2.0 or higher. A "D" (1.0) is considered passing for a course, but a student's CGPA must not be below 2.0, or they will be placed on academic probation or suspension. Additionally, students must have successfully completed (received As, Bs, Cs, or Ds) sixty-seven percent (67%) of all courses attempted in the program (Percentage of Credit Completion-PCC).

» Master's and Graduate Certificate students are required to maintain a cumulative GPA of 3.0 (B) or higher for all graduate-level coursework applying toward the degree. While a "C" grade is considered passing, it will impact a student's CGPA. A letter grade of "D" is not passing for graduate-level programs and will require the student to retake the course. Additionally, students must have successfully completed (received As, Bs, or Cs) sixty-seven percent (67%) of all courses attempted in the program. (Percentage of Credit Completion-PCC).

Academic Progress and Veteran Affairs Educational Benefits

Students using Veteran education benefits are required to maintain Satisfactory Academic Progress (SAP).

Academic Probation

EC-Council University makes a discerned effort to monitor student progress on a continual basis. A significant part of this monitoring process is to review the student's Cumulative GPA (CGPA) every term. Every student admitted to EC-Council University is expected to maintain SAP.

Students who fail to meet the Qualitative or Quantitative guidelines at the end of the term/period of review are automatically placed on a warning status for one term and notified of the status. The student continues to receive federal financial aid for this term. If at the end of the term/period of review, the student is now meeting all Satisfactory Academic Progress standards, the warning status is removed, and the student is now in good standing.

Failure to maintain SAP in any given term will result in the student being placed on academic probation and at risk of suspension. A student who does 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 in improving their GPA.

Requirements for Students on Academic Probation

Bachelor's Students

Students are required to improve their CGPA the first term they are on Academic Probation. Students who have made improvements, but have not raised their CGPA to the required 2.0, will remain on academic probation for each subsequent term until achieving the required 2.0 CGPA. To maintain SAP, the student is required to make SAP and GPA improvements each term. Therefore, students are required to earn As, Bs, or Cs each successive term while on AP to maintain a successful completion (67%) of all courses attempted in the program (Percentage of Credit Completion-PCC).

Master's and Graduate Certificate Students

Students are required to improve their CGPA the first term they are on Academic Probation. Students who have made improvements, but have not raised their CGPA to the required 3.0 will remain on academic probation for each subsequent term until achieving the required 3.0 CGPA. To maintain SAP, the student is required to make SAP and GPA improvements each term. Therefore, students are required to earn As or Bs each successive term while on AP to maintain a successful completion (67%) of all courses attempted in the program (Percentage of Credit Completion- PCC).

Satisfactory Academic Progress Review

Students on academic probation will have their records reviewed each term. Once the student has returned to SAP, the student will be removed from academic probation. A formal notice will be sent to the student via email from the Registrar. A copy of this notice will become part of the student's permanent file.

Academic Suspension

A student that does not maintain SAP (2.0 cumulative GPA for undergraduate students and 3.0 cumulative GPA for graduate students and a 67% course completion) upon their return from academic suspension will be terminated and may not continue enrollment. Students may appeal the decision for an academic suspension to the Dean.

The suspension will be based on a number of factors, including (but not limited to) the number of failing grades, past academic performance, level of academic deficiency, and student's probability of success. Notice of academic suspension will be sent to the student by the Registrar and will become part of the student's permanent record.

Students suspended from the program are terminated unless the following occurs:

» The student files an appeal and submits it to the school's Registrar at registrar@eccu.edu.
» The academic appeals board (consisting of the Dean, Registrar, and Compliance Coordinator) review the appeal. Special circumstances are identified to warrant and grant the student's appeal.

The appeal of Probation and/or Suspension

Students who have been suspended 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 suspension decision.

Students have the right to appeal all academic probation or suspension 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 academic appeals board (consisting of the Dean, Registrar, and Compliance Coordinator) will review the academic probation or suspension. Within 15 days of receiving the student's appeal, the Dean shall render a final decision and notify the student.

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 (please use the table on page 66) 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. A grade of a "D" is not considered a passing grade for graduate students PCC must be 67% or 2 out of every three courses attempted must be successfully completed.

Maximum Time of Completion

The student's maximum time of completion for their program of study shall be one and a half times the program length. This equates to 150% of the attempted credit hours designated in the program outline. The MSCS program consists of 36 credits, so the students' maximum time of completion shall be 54 attempted credit hours (36 X 150%). The BSCS program consists of 60 credits, so the students' maximum time of completion shall be 90 attempted credit hours (60 X 150%), this equates to a percentage completion rate of 67% (36/54 and 60/90).

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 a certain 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 severe 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: 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
Cyber Bullying	» Bullying that takes place using electronic technology
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 the faculty do not approve such collaboration

EC-Council University will act 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 the Dean's file of all instances of academic dishonesty for the institution.

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

- 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.
- Once the student 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 to 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.

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% of original work. Any work submitted that contains more than 25% unoriginal work regardless of whether the sources are appropriately cited may be considered a violation of the academic honesty policy, depending on the nature of the assignment, and consent of the assigned instructor.

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 acknowledgment 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 their 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.

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 credentials.

» EC-Council University implements student identity verification in several ways to ensure proper ID.

- » A Valid Government issued ID is required with admissions application along with a photo of yourself (selfie) holding your official government ID.
- » Login credentials are required for the online LMS portal.
- » Proctored exams require a valid photo ID to be presented at the time of exam as well as a screenshot of ID.

ProctorU Exams

» EC-Council University utilizes ProctorU exam proctoring services for all courses which require a final exam. These exams are presented throughout the program.

» This secure cloud-based proctoring service allows students to take secure exams at their convenience while maintaining University integrity.

» The exam can be accessed through Canvas. More instructions and training videos for utilizing ProctorU can be viewed in the New Student Orientation, student handbook, or by going to ProctorU's website at https://www.proctoru.com/. A PC or Mac, webcam (external or built-in), and an internet connection are required.

The following courses require a proctored exam: CIS 304, CIS 308, CIS 402, CIS 405, CIS 408, ECCU 501, ECCU 504, ECCU 507 and MGMT 502.

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 the grade point average (GPA).

Grade Point Average Calculation

The calculation of the students' Grade Point Average or GPA will be the total number of credits per course (3) multiplied by the grade points earned divided by the total number of credits earned. Transfer credits are not included in GPA calculations.

Bachelor's Grading Scale

LETTER GRADE	RANGE OF POINTS	GRADE POINTS
A	93.00-100.00	4.00
A-	90.00-92.99	3.67
B+	87.00-89.99	3.33
B	83.00-86.99	3.00
B-	80.00-82.99	2.67
C+	77.00-79.99	2.33
C	73.00-76.99	2.00
C-	70.00-72.99	1.67
D+	67.00-69.99	1.33
D	60.00-66.99	1.00
F	0.00-59.99	0.00
W	Withdrawal from a **course**	
AW	Administrative Withdrawal	
I	Incomplete	
IP	In Progress	
R	Retaken Course	

Master's/Graduate Certificate Grading Scale

LETTER GRADE	RANGE OF POINTS	GRADE POINTS
A	93.00-100.00	4.00
A-	90.00-92.99	3.67
B+	87.00-89.99	3.33
B	83.00-86.99	3.00
B-	80.00-82.99	2.67
C+	77.00-79.99	2.33
C	73.00-76.99	2.00
C-	70.00-72.99	1.67
F	0.00-69.99	0.00
W	Withdrawal from a course	
AW	Administrative Withdrawal	
I	Incomplete	
IP	In Progress	
R	Retaken Course	

GRADING SYSTEM

I An Incomplete "I" is a temporary grade that may be given at EC-Council University's discretion to a student when illness, necessary absence, or other reasons beyond the control of the student prevents completion of course requirements by the end of the academic term.

To qualify for an "Incomplete," the student must meet all of the below criteria:

- Attendance has been satisfactory through at least 60% of the term;
- Currently on track to complete the course with a passing grade;
- Required work may be reasonably completed in an agreed-upon time frame;
- Able to document an extenuating circumstance that hindered progress in the course
- The Incomplete is not given as a substitute for a failing grade;
- The Incomplete is not based solely on a student's failure to complete work or as a means of raising his or her grade by doing additional work after the grade report time;
- The student initiates the request for an incomplete grade before the end of the last week of the course;

Appropriate grades must be assigned in other circumstances. A failing grade and the last date of attendance should be recorded for students who cease attending class without authorization. Students who are unable to complete a course and who do not meet these circumstances should consider withdrawing from the course.

The following provisions for incomplete grades apply:

- It is in the student's best interest that Incomplete grades be made up by the agreed-upon completion date. Incomplete grades must be made up, and final grades submitted within 21 days from the date the Incomplete was recorded.
- The course work may be completed while the student is not enrolled.
- Incomplete grades do not affect the grade point average.
- After 21 days past approval of the Incomplete, if the work is not submitted/graded, the grade assigned will be based on the cumulative points earned
- and affect GPA.
- An Incomplete grade may not be considered passing for purposes of determining academic standing, federal financial aid eligibility, or other purposes.

IP In Progress applies to currently enrolled courses.

R Retaken course. An "R" grade is indicated on the transcript when a later grade has superseded the course grade. Only the latter 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 a withdrawal is allowed.

GRADING SYSTEM

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

Lack of Attendance/Participation

During the first two weeks of class, students who fail to participate (turning in an assignment, discussion post, etc.) without contacting the faculty member and making special arrangements may 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.

Failure to participate in a given week's work will result in the student being placed on Attendance Probation, and they will have one week to show participation. A failure to participate during Attendance Probation will result in the student being placed on Attendance Suspension, and they will have one week to show participation. A failure to participate during Attendance Suspension will result in course withdrawal retroactive to the last date of recorded 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

The calculation of the students' Grade Point Average or GPA will be the total number of credits per course (3) multiplied by the grade points earned divided by the total number of credits in which a grade of A, B, C, D, or F has 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- = 2.67 grade points x 3 credit hours = 8.01
» ECCU 502 C+ = 2.33 grade points x 3 credit hours = 6.99
» ECCU 503 A = 4.00 grade points x 3 credit hours = 12
» ECCU 504 B+ = 3.33 grade points x 3 credit hours = 9.99
» ECCU 505 A- = 3.67 grade points x 3 credit hours = 11.01

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 a course or project requirements.

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

Honors Lists

After the end of each term, all students in degree-seeking programs who earned a high GPA for the term will be recognized for their high achievement.
Those students who have earned a 3.75 to 4.0 GPA for the term are placed on the President's List.
Those students who have earned a 3.25 to 3.749 GPA for the term are placed on the Dean's List.

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.

Grounds for a Grade Appeal

The following are grounds for an informal or formal grade review.

» The faculty member of record inaccurately calculated the student grade.

» The faculty member of record determined a grade using a process different from that identified in the grading rubric or in a written change to that grading rubric distributed to students by a means determined by the faculty member.

» The faculty member of record applied an inconsistent grading standard within the course.

» The faculty member of record violated a written agreement with the student.

» The faculty member of record violated an institutional policy in assigning coursework, administering exams, and in assigning grades.

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 specific responsibilities toward my fellow distance learners, my institution, and myself. To fulfill these responsibilities, I pledge adherence to this Code of Conduct.

I will fully observe 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 institutional 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.

RIGHTS AND RESPONSIBILITIES

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 by 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:

1. The action was taken against the student in accordance with the University's disciplinary procedures

2. A decision of the faculty, based on the student's academic performance

3. Non-payment of fees, in accordance with the University's regulations on payment of fees.

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 Student 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:

1. Encourages Informal Resolution

2. Is fair and efficient

3. Treats the students with appropriate seriousness and sympathy

4. 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 services by the University." Examples include but are not limited to:

1. Inaccurate or misleading information about programs of study

2. Inadequate teaching or supervision

3. Insufficient academic facilities

4. Service not provided to standard advertised

5. The behavior of a member or staff

6. 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.

RIGHTS AND RESPONSIBILITIES

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 typical 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 can be found 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 at: dean@eccu.edu, 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.

What can I do if I'm still not satisfied?

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, 2044 Galisteo Street Suite 4, Santa Fe, NM 87505-2100, 1-505-476-8400 or https://hed.state.nm.us/students-parents/student-complaints From the NMHED website: The Private Postsecondary Schools Division (PPSD) is responsible for the following:

- Enforcing the New Mexico statutes and rules for all private postsecondary educational institutions operating with a physical presence in the state of New Mexico
- Cooperating with authorities seeking to resolve student complaints against state-authorized postsecondary educational institutions and designated out-of-state proprietary schools

UNIVERSITY RIGHTS AND RESPONSIBILITIES

The National Council for State Authorization Reciprocity Agreements (NC-SARA) is an agreement among member states, districts and territories that sets national standards for interstate offering of postsecondary distance education courses and programs. EC-Council University (ECCU) is an NC-SARA approved institution, and the New Mexico Higher Education Department (NMHED) is the NC-SARA Portal Entity for New Mexico. Distance Education students attending ECCU who would like to resolve a grievance should follow ECCU's established Student Complaint Process. However, if an issue cannot be resolved internally, you may file an NC-SARA complaint with the New Mexico Higher Education Department. Complaints regarding grades and student conduct violations shall not be reviewed by NMHED. Please visit https://hed.state.nm.us/students-parents/nc-sara for more information.

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

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 affecting 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 to be 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. Another 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. FERPA does not cover individuals who applied to the school but did not attend. 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. A 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@eccu.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 outlined in Section 504 of the Rehabilitation Act, the Americans with Disabilities Act (ADA) Amendments Act (ADAAA), 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

Students must demonstrate that their need for academic adjustments or other reasonable accommodation is based solely on their permanent disability, After a student submits their documentation, the Student Support Manager will determine eligibility as well as appropriate and reasonable accommodations Students need to repeat their request for services every term.

Steps

1. Submit documentation via email, mail, or fax to 505-856-8267.
2. The Student Support Manager will contact the student to set up an intake appointment via email.
3. Student Support Manager determines appropriate accommodations.
4. Accommodations will begin within five business days after intake appointment whenever possible.

Confidentiality

Services provided are confidential. ECCU does not release information to any persons or agencies without the written consent of the student. Information may be released pursuant to a subpoena or under circumstances that might pose a danger to the student or others, in situations of suspected child abuse, or under circumstances where ECCU officials have a need to know.

Evaluative Documentation

As the first step in the initiation of services, students requesting are required to submit documentation of a disability to verify eligibility under the Americans with Disabilities Act Amendments Act (ADAAA), Section 504 of the Rehabilitation Act of 1973. ADAAA defines a disability as a substantial limitation of a major

life function. The diagnostic report must document a disability. It is essential to recognize that academic adjustment needs can change over time and are not always identified through the initial diagnostic process. Conversely, a prior history of accommodation, without demonstration of current need, does not in and of itself warrant the provision of a like accommodation.

Those students with no documentation and suspecting they may have a disability may seek an evaluation from community diagnosticians or health care providers. The cost of the evaluation is the responsibility of the student, so please check with your health insurance to see if any of the cost is covered through your health insurance policy.

Documentation must

» Verify a disability; the ADAAA defines a disability as a substantial limitation of a major life function.

» Include a specific diagnosis which describes the nature of the permanent disability and its functional limitations in an academic environment as well as other university settings.

» Include specific recommendations for academic adjustments or accommodations. Academic adjustment needs can change over time and are not always identified through the initial diagnostic process. A prior history of accommodation, without demonstration of current need, does not in itself warrant the provision of a similar accommodation.

» Be signed by the medical or mental health professional or diagnostician.

» Be timely and typed/written on professional letterhead stationery.

» Be given to the Registrar who will begin the intake process.

Documentation may include

» Letter from doctor

» ECCU Diagnosis Verification Request Form

» DSM diagnosis

» Psychological evaluation

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 long lead time, regular mail service may be an alternative.

RIGHTS AND RESPONSIBILITIES

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.

FINANCIAL ASSISTANCE

Corporate Reimbursement

EC-Council University is accredited; therefore, tuition is eligible for many corporate tuition reimbursement plans. Our student advisors will be happy to work with your company to provide the necessary documentation of academic progress to facilitate reimbursement or payment of tuition under such programs. Please refer to your company's benefits policy for the most up to date details.

Veterans Benefits

Bachelor's and Master's degree and graduate certificate programs are eligible for VA Education Benefits. For complete information on using your benefits, please visit www.vets.gov

The GI Bill ® covers all online education programs taken as part of an EC-Council program. Distance housing allowance rates are also an applicable benefit. "GI Bill®" is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government website at www.benefits.va.gov/gibill.

Navigate to www.vets.gov/education/apply/ to apply for your benefits and get your "Certificate of Eligibility." Once you are admitted to EC-Council University, our admissions team will help ensure you submit all necessary documents.

Any Veteran that is eligible to use VA Educational Assistance and wishes to attend or participate in the course of education during the period beginning on the date on which the individual provides the educational institution a certificate of eligibility (COE) for entitlement to educational assistance. There will not be any penalty, including the assessment of late fees, the denial of access to classes, libraries, or other institutional facilities, or the requirement that the VA eligible student borrows additional funds, on financial obligations to the institution due to the delayed disbursement of funding from the VA.

Title IV Federal Student Financial Assistance

EC-Council is not currently approved by the US Department of Education as an eligible Title IV institution. While we do not currently participate in Title IV funded student loan programs, no-interest institutional payment plans are available.

Monthly Payment Plans

EC-Council University offers monthly payment plans that divide the tuition into three equal payments. The initial payment is paid before the start of the first class of the term, and the subsequent two payments are due mid-month (15th) the first and second month of the term. There is no interest charged for this payment plan. Good standing on payment plans will ensure continued eligibility for program participation.

FINANCIAL ASSISTANCE

University Scholarships

EC-Council University provides direct tuition assistance through the provision of scholarships. These programs are directed to specific eligibility criteria that are merit-based on diversity criteria, background experience, prior academic achievement and excellence, industry leadership recommendation, and/or submitted writing essays. At a minimum, all criteria for admissions to a program of study at the university must be met to be deemed eligible for any scholarship funds. As scholarship funding is limited, merit criteria basis and adherence to established scholarship program application deadlines will determine actual awards. Example programs include:

» Cyber Challenge
» The Cyber Security Dean's Scholarship
» New Mexico Scholarship
» The Cyber Security Heroes Scholarship
» Associate's Cyber Security Scholarship
» Women in Cyber Security Scholarship
» EC-Council Foundation Fellowship

For a full list of scholarships and programs, visit: https://www.eccu.edu/?s=scholarships

Tuition payment is the responsibility of a student; if alternative sources of funding are not qualified for, the student remains responsible for tuition payment.

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.

Bachelor's Program Tuition

The total cost estimate is based on completing 60 credit hours with tuition rates, plus required fees.
To be considered full-time in the Bachelor of Science in Cyber Security program, students must be enrolled and complete at least 9 credits per term.

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

*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.

Tuition Costs
$465 **Per Credit Hour**
Application Fee: $200
Technology Fee: $50 per term
iLabs Fee: $50 per certification course
Graduation Fee: $150
Transcript Fee: $10+shipping**
Transcript w/Apostille: $20+shipping**

**Students must have all financial obligations met prior to transcripts being released.
ECCU reserves the right to withhold transcripts and other similar documents when students, for example, have unmet obligations to ECCU.

PROGRAM COSTS AND PAYMENT

Master's and Graduate Certificate Programs

The total cost estimate is based on completing 36 credit hours (MSCS) or 9-15 credit hours (Graduate Certificate) with tuition rates applied based on the student's government photo ID plus required fees. To be considered full-time, students must be enrolled and complete six credits (2 courses) per term and three credits per term is considered half-time for the Master of Science in Cyber Security program or Graduate Certificate program.

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

*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.

Tuition Costs
$540 **Per Credit Hour**
Application Fee: $200
Technology Fee: $50 per term
Graduation Fee: $150
iLabs Fee: $50 per certification course
Transcript Fee: $10+shipping**
Transcript w/Apostille: $20+shipping**
Specialization: Security Analyst **Exam Fee: $999**
Specialization: Executive Leadership in Information Assurance **Exam Fee: $999**

**Students must have all financial obligations met prior to transcripts being released.
ECCU reserves the right to withhold transcripts and other similar documents when students, for example, have unmet obligations to ECCU.

PROGRAM COSTS AND PAYMENT

Fees

Application Fee*

There is a $200 application fee for all student applicants. 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. The application fee may be waived at the discretion of the University.

Registration Fee*

There is a one-time per program $200.00 registration fee. The fee will be assessed to all Bachelor's, Master's, and Graduate Certificate Program this will also include non-degree.

Tuition (Course Fee/Credit Hour)

- Master's and Graduate Certificate Program: $540/credit hour
- Bachelor's Program: $465/credit hour

Lab Fee* $50 (Course Fee) ECCU 500, ECCU 501, ECCU 502, ECCU 503, ECCU 506, ECCU 510, ECCU 513, ECCU 522, and ECCU 523.

All courses accompanied by a lab will be assessed with a lab fee of $50.

*These are non-refundable registration fees.

PROGRAM COSTS AND PAYMENT

Technology Fee*

A technology fee of $50 is due each term the student is enrolled.

Prior Learning Assessment Fee*

There is a Prior Learning assessment fee of $50 per credit hour.

WebAssign for MTH 350

MTH 350 – Introduction to Statistics requires a proctored exam. Students are required to obtain a WebAssign access code and use the course key that the instructor will provide to sign up for WebAssign (http://www.webassign.net/). The access code will allow students to access WebAssign, which is the platform by which all homework and quizzes will be submitted.

Graduation Fee* $150

A Graduation Fee of $150 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 Registrar verifies a student's graduation application, the earned degree will be conferred and sent along with two (2) official transcripts, congratulatory letter, diploma, and memorabilia in the graduation packet.

Official Transcript Fee $10* (+$150 shipping , if mailed outside of the USA)

Forms are available online at www.eccu.edu. Please send a completed form to the Registrar at registrar@eccu.edu. Official transcripts can also be requested in your Populi student portal. Contact the Registrar at registrar@eccu.edu for additional questions about requesting an official copy of your transcript.

Tuition and fees 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.

*These are non-refundable registration fees.

REFUND POLICY

Cancellation of Enrollment Agreement

The student has five days after signing the enrollment agreement, prior to the beginning of the term, 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.

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 is withdrawn prior to the predetermined deadline. A student may withdraw from a course or program by notifying the Registrar in a documented manner (withdrawal form, mail, e-mail, or fax). 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. Application and registration fees are non-refundable. The percentage of tuition minus the application and/or registration fees are returned to the student after each week based on the schedule below and are calculated on a per-class basis.

WEEK WITHDRAWN	PRORATED TUITION CHARGE	TUITION REFUND (IF APPLICABLE)
Through the 1st Week	0%	100%
2nd Week	20%	80%
3rd Week	30%	70%
4th Week	40%	60%
5th Week	50%	50%
6th Week	60%	40%
7th Week	70%	30%
8th Week	80%	20%
9th Week	90%	10%
10th Week	100%	0%

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

REFUND POLICY

Examples (in USD)

» Bob began class in the Bachelor's program and paid tuition for a 3-credit class with a lab fee, totaling $1,445. Three days later, he withdrew from the Cyber Security program. He received a full refund of $1,445 because he withdrew during the "5-day cooling-off period."

» Sally returned her Student Enrollment Agreement for the Master's program and paid tuition for a 3-credit class with lab and technology fees, totaling $1,720. 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 100% refund of the tuition. Sally received a refund of $1,670.

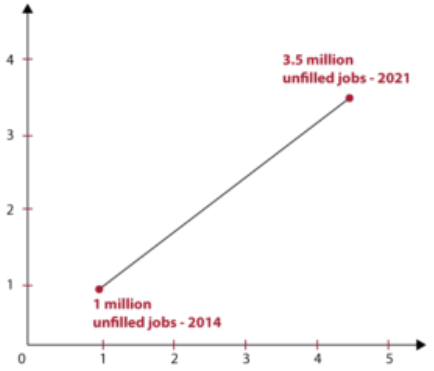
Special Circumstances

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 Manager of Finance.

Join the Cyber Security Advancement Alliance by EC-Council University

What is the Cyber Security Advancement Alliance All About?

Since EC-Council's inception, we have continuously overhauled and reprioritized our cybersecurity programs to meet the demand and requirements of the industry, government, and education. The world, however, is continuously in a crisis mode. A Cyber crisis mode. The number of jobs that are being created in cyber is growing at a staggering rate, and the fact is that Universities across the globe are unable to produce a capable and reliable cyber workforce at the speed that the marketplace requires



The shocking fact is that the cybersecurity community has been unable to reduce the inefficiencies of the cybersecurity workforce, unlike the other tech sectors. As a result, cybercrime is growing at an alarming rate.

As a responsible educator, EC-Council University is calling on industry partners to join its Cyber Security Advancement Alliance to help reverse this problem. Our goal is to ensure that with the input of the industry, we will be able to solidify, improve, and innovate advanced cybersecurity learning programs that are affordable. Further that they provide opportunities for the development of a technology workforce of our Alliance members so that they meet emerging cybersecurity requirements of the industry. With the support of our Alliance members, we aim to continue to innovate hand in hand with the needs of employers.

How Do We Plan to Contribute to the Community?

With the support of our Alliance Partners, we plan to contribute to the community in the following ways:

1. Monthly Expert Sessions:
From cybersecurity practitioners across the world, which will be made available as webinars to everyone without any fee.

2. Industry Engagement Sessions:
We plan to invite our members to contribute through Advisory Boards and other forums to the enhancement and development of our cyber programs to ensure that they are relevant to the needs of the industry.

3. Events and Conferences:
We will invite community members to our various events across the globe so that a proper dialogue can be held for the betterment of the industry.

4. Applied Research:
Students will be encouraged to utilize applied research projects in their coursework that support workplace challenges through various methods such as internships, capstone projects, and case studies.

5. Scholarships:
EC-Council University will support 10% tuition scholarship opportunities for member's employees as well as their spouses and children. Plus, members will have access to additional scholarship awards exclusive to advisory board recommendations. Application fees will also be waived.

CYBER SECURITY ADVANCEMENT ALLIANCE

How Can Your Organization Benefit

When you join our Cyber Security Advancement Alliance program, members receive:

» 10% Tuition Scholarship of up to $2000.00 per program (Master's degree, Graduate certificate, or Bachelor's degree) applied by the course. (Available for member employees, spouses and children)
» Application costs waived.
» Exclusive access to additional scholarship programs.
» Expedited and customized payment plans that support organizational tuition assistance programs.
» Applied project assignments (and internships where applicable) that support your working environment and academics.
» Graduate and undergraduate joint research fellowship opportunities.
» Preferential organizational leadership representation on University Advisory Boards that steer the curriculum to meet the needs of a well-trained cyber workforce.
» Motivation for academic success as the merit nature of the scholarship is based on maintaining satisfactory academic progress.

Build a Future Through Research Fellowship and Scholarship

With the Cybersecurity Advancement Alliance program at ECCU, companies and organizations can enhance members and their families' lives with education. More than an employee benefit, education is a strategic investment that will give your organization the edge needed to thrive in today's economy.

The Cyber Advancement Alliance seeks to bridge the gap in government/industry and education collaboration to produce better partnering on the ideas, trends, and outcomes needed for an expanding and higher quality cybersecurity talent pool.

Organizations, associations, municipalities, and other agencies can give members and employees a Cybersecurity Advancement Alliance Scholarships benefit through EC-Council University

A leader in online cybersecurity academic excellence, EC-Council University provides flexible degree and certificate programs designed to move adult learners forward in their careers. With a dedicated faculty and staff, we also offer exceptional service to help students reach their education goals.

Become a Cybersecurity Advancement Alliance member and invest in the future of your team with EC-Council University!

CYBER SECURITY ADVANCEMENT ALLIANCE

How Can Your Organization Benefit

When you join our Cyber Security Advancement Alliance program, members receive:

» 10% Tuition Scholarship of up to $2000.00 per program (Master's degree, Graduate certificate, or Bachelor's degree) applied by the course. (Available for member employees, spouses and children)
» Application costs waived.
» Exclusive access to additional scholarship programs.
» Expedited and customized payment plans that support organizational tuition assistance programs.
» Applied project assignments (and internships where applicable) that support your working environment and academics.
» Graduate and undergraduate joint research fellowship opportunities.
» Preferential organizational leadership representation on University Advisory Boards that steer the curriculum to meet the needs of a well-trained cyber workforce.
» Motivation for academic success as the merit nature of the scholarship is based on maintaining satisfactory academic progress.

Build a Future Through Research Fellowship and Scholarship

With the Cybersecurity Advancement Alliance program at ECCU, companies and organizations can enhance members and their families' lives with education. More than an employee benefit, education is a strategic investment that will give your organization the edge needed to thrive in today's economy.

The Cyber Advancement Alliance seeks to bridge the gap in government/industry and education collaboration to produce better partnering on the ideas, trends, and outcomes needed for an expanding and higher quality cybersecurity talent pool.

Organizations, associations, municipalities, and other agencies can give members and employees a Cybersecurity Advancement Alliance Scholarships benefit through EC-Council University

A leader in online cybersecurity academic excellence, EC-Council University provides flexible degree and certificate programs designed to move adult learners forward in their careers. With a dedicated faculty and staff, we also offer exceptional service to help students reach their education goals.

Become a Cybersecurity Advancement Alliance member and invest in the future of your team with EC-Council University!

OUR PARTNERS

EC-COUNCIL UNIVERSITY BOARD OF DIRECTORS

Sanjay Bavisi

CEO, EC-Council Group & Chairman of the Board, EC-Council University, LLB (Hons), Middle Temple [United Kingdom] Mr. Bavisi is the co-founder and president of EC-Council International, Ltd., an international corporation, that is ANSI accredited and widely recognized for its member-based and partner-based structure and its certification of information assurance professionals around the world.

George Sehi

Doctorate in Academic Administration, Southern Illinois University at Carbondale; Master of Science in Thermal & Environmental Engineering, Southern Illinois University at Carbondale; Bachelor of Science in Civil Engineering, Southern Illinois University at Carbondale

David Leasure

Leasure has earned bachelor's, master's, and doctoral degrees in computer science and was associate professor of computer science at Texas A&M University Corpus Christi.

Eric Lopez

Eric Lopez earned his BS degree in New Mexico State University. Eric is the executive director of the EC-Council Foundation, which delivers IT Security Conferences all over the world.

Lata Bavisi

President EC-Council University. Over a span of 20 years, Lata Bavisi has had a very exciting career with experiences in different industries across the globe. As a trained attorney, she has been able to help steer many of these organizations. These roles manifested into leadership positions which benefited the organizations greatly as she played a pivotal role to help corporate growth.

Kim Sassaman

Master's Degree, Computer & Information Systems Security/ Information Assurance, Norwich University; Bachelor of Science, Information Assurance & Security, Capella University

David Oxenhandler

Master of Business Administration, University of Massachusetts; Bachelor of Science, Business, University of Connecticut

EC-COUNCIL UNIVERSITY BOARD OF DIRECTORS

EC-Council University Advisory Council

Roxanne Kemp, PhD

Chairperson of Advisory Council Doctor of Philosophy - PhD, Technology, Capitol Technology University; Master in Liberal Studies -Psychology Tarleton State University.

Wesley Alvarez

Bachelor of Science, Business Commerce, Niagara University; Associate of Science, Business Administration, Monroe Community College

Albert Whale

Bachelor of Science, Electrical Engineering, Penn State University

Kevin Cardwell

Master of Science, Software Engineering, Southern Methodist University; Bachelor of Science, Computer Science, National University.

Stephen Miller

Master of Science / Master of Information Security in Managing Computer Technology, Houston Baptist University

Gregory Carpenter

Doctorate of Public Health (ABD), Walden University; Master of Science, Seton Hall University; Bachelor of Science, Colorado Christian University -Nitin Gaur Master of Business Administration, University of Maryland University College; Master of Science, Management Information Systems, University of Maryland University College

Nitin Gaur

Master of Business Administration, University of Maryland University College; Master of Science, Management Information Systems, University of Maryland University College

EC-COUNCIL UNIVERSITY STAFF

Lata Bavisi
President EC-Council University

Roxanne Kemp, PhD
Dean - Chief Academic and Administrative Leader

Bunny Martinez
University Registrar

Alexis Gonzales, AS
Administrative Assistant for Academic Operations

John Hilger, BS
Director of Compliance

Mark Chavez, MSW
Bursar

EC-COUNCIL UNIVERSITY STAFF

David Valdez

Student Success & Academic Support Executive

Zanna Jones

Academic Support Advisor

Lisa "Elle" Ligon

Enrollment Advisor & Faculty Member

Sarah A. Elliott

Enrollment Advisor

FACULTY

Charline F. Nixon, DM, PhD
Faculty Member

Doctor in Management, Fr. Urios University; Doctor in Philosophy, Fr. Urios University; Master in Cybersecurity, Virginia College Online; Master in Business Administration, Fr. Urios University; Graduate Certificate in Information Assurance; Bachelor of Science in Commerce, Fr. Urios

Yuri Diogenes, MS
Faculty Member

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.

Sandro Tuccinardi, JD
Faculty Member

Juris Doctorate, McGill University; Master of Science, Computer Science, Dalhousie University; Bachelor of Arts, Social Science, University of Ottawa

Yakov Goldberg, MS
Faculty Member

Master of Science in Information Assurance, Capella University; CISSP, GIAC, and CompTIA Sec+ and Net+

David Moured, PhD
Faculty Member

Doctor of Philosophy, Computer Information Systems, Nova Southeastern University; Master of Science, Network Security, Capitol College, Bachelor of Science, Business Information Systems, Villa Julie College, CISSP, C|CISO, C|EH, C|HFI, C|ND, C|NDA, CompTIA Linux+, Certified Reverse Engineering Analyst, E|CSA, LPIC-1, L|PT

Danielle Babb, PhD
Faculty Member

Doctor of Philosophy in Organization and Management, Information Technology Management specialization, Capella University, Master of Business Administration, Information Systems Emphasis, University of Redlands, Bachelor of Science, Business Administration, University of California at Riverside.

Pamela Garrett, MBA
Faculty Member

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

Warren Mack, PhD
Faculty Member

Doctor of Philosophy in Vocational and Technical Education, Virginia Tech; MS – Technology Education, Central Connecticut State University; BS-Industrial Arts Education, State University of New York at Oswego

Willie Session, MBA
Faculty Member

Doctor of Philosophy Candidate in Public Policy and Administration, Walden University; Master Business Administration, National University; Bachelor of Science, Southern Illinois University

FACULTY

Oluwaseyi Ojo PhD, CEng *Faculty Member*

Doctor of Philosophy in Cybersecurity and Risk Management, Trinity International University
Master of Business Administration (M.B.A.), Business School Netherlands

Brian McDaniel, MS
Faculty Member

Doctor of Information Assurance Candidate, University of Fairfax, Master of Science in Cybersecurity, EC-Council University
Master of Science in Computer Science, Oklahoma City University

Elgrie J. Hurd III, MA, MS
Faculty Member

Doctor of Philosophy in Psychology Candidate
Master of Science in Psychology, Grand Canyon University; Master of Arts in Sociology, San Jose State University

Alex Lazo, PhD
Faculty Member

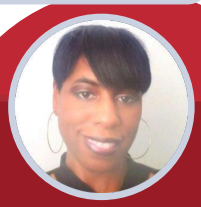
Doctor of Philosophy in Organization and Management with an emphasis in IT Management, Capella University;
Masters of Science in Management Information Systems and a Bachelor or Arts in International Business from California State University, Fullerton.

Christopher McDonald, MBA
Faculty Member

Doctor of Philosophy Candidate in Technology, Capitol Technology University; Master of Business Administration from Saint Leo University

Julie Beck, MS
Faculty Member

Master of Science in Cyber Security, EC-Council University; Master of Science in Information Technology, Kennesaw State Unbiversity



Taneise Polk, MS
Faculty Member

Master of Education in Instructional Technology, Texas Tech University; Bachelor of Science in Interior Design

Arnold Webster, MS
Faculty Member

Master Degree in Computer Science, City University Seattle;
Graduate Certificate, Change Leadership, City University of Seattle; Master of Science Governmental Information Leadership, CIO Concentration, National Defense University

Shena Young, MS
Faculty Member

Master Degree in Information Technology, American InterContinental University; PMP Certification, ITIL Foundation V2 and V3 Certified, ITIL Service Capability: Operational Support and Analysis Certification, ITIL Service Capability: Service Offerings and Agreements, ITIL Service Capability: Planning, Protection, and Optimization Certification, ITIL Service Capability: Release Control and Validation Certification, HDI Support Center Manager Certification, A+ Certification, Six Sigma Green Belt Certified, Six Sigma Lean trained

Copyright

EC-Council University follows the copyright law of the United Stateswhichprohibitsthemakingorreproductionofcopyrightedmaterialsexceptunder 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 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 July 1, 2020, and December 31, 2021. Students inactive (not enrolled) for one calendar year must be readmitted and will move forward to the current catalog 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 vast 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 employing 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