



The Leader in Cybersecurity Education

EC-COUNCIL
UNIVERSITY

ACCREDITED. FLEXIBLE. ONLINE.

CATALOG 2018

Effective July 2018 – December 2018

TABLE OF CONTENTS

Table of Contents	02	English Requirements for International Students	15	Graduate Certificate Program Requirements	50
Chariman's Message	04	Technology Requirements	16	Testing for EC-Council Certifications	52
THE UNIVERSITY	05	International Student Admission & Visa Services	17	STUDENT SERVICES	53
Mission Statement	05	Student Enrollment Agreement	17	Student Services Portal	53
University History	05	Academic Services	17	Registering for Courses	53
Institutional Values	05	PROGRAM ADMISSION REQUIREMENTS	18	Mode and Duration of Study	53
Licensure	05	Bachelor's Program	18	Course Delivery	53
CNSS Standards	05	Master's Program	18	Credits	54
National Institute of Standards & Technology	06	Graduate Certificate Program	18	Grades	54
Accreditation	06	TRANSFERRING CREDIT	20	Textbooks	54
University Contact Information	07	Course Transfer Credits	20	ACADEMIC POLICIES AND GUIDELINES	55
Institutional Goals and Objectives	08	Prior Learning Portfolio	20	Academic Load	55
ACADEMIC CALENDAR	09	Maximum Allowable Transfer Credit	22	Minimum Academic Achievement	55
Dates and Deadlines	09	Transferability of ECCU Credit	22	Maximum Program Length	55
2018 Holidays	09	PROGRAMS OF STUDY	23	Attendance and Participation	55
2018 COURSE OFFERINGS	10	Bachelor of Science in Cyber Security	24	Missed or Late Assignments	55
Bachelor's program	10	Bachelor's Degree Graduation Requirements	25	Leave of Absence	56
Master's Program	11	UNDERGRADUATE LEVEL COURSES	26	Satisfactory Academic Progress	56
ADMISSION REQUIREMENTS	12	Master of Science in Cyber Security	34	Academic Probation	57
Application Procedure	12	Master's Degree Graduation Requirements	35	Academic Suspension	58
Applicants w/degree from non-US institution	12	GRADUATE LEVEL COURSES	37	Appeal of Probation and/or Suspension	58
Admission	13	Graduate Certificate Program	49	Cumulative Grade Point Average (CGPA)	59
				Percentage of Credit Completion	59

TABLE OF CONTENTS

Maximum Time of Completion	59	Third Parties	70	ECCU Staff	85
ACADEMIC HONESTY POLICY	60	Rights Reserved	70	ECCU Faculty	86
Course Policies on Cheating & Plagiarism	60	STUDENT RECORDS/RIGHT OF PRIVACY	71	Copyright	88
Citing Sources	61	Directory Information	72	The Catalog	88
Original Content	61	Non-Directory Information	72		
Timeline	61	Electronic Files	72		
Student Identity Verification	61	Access to Records	72		
Remote ProctorNOW Exams	61	Disability	73		
GRADING SYSTEM	62	Student Rights	74		
GPA Calculation	62	Anti-Harassment	75		
Credits	65	Non-Discrimination	75		
Grade Appeal	65	FINANCIAL ASSISTANCE	76		
Withdrawal From Program or Course	65	University Scholarships	77		
RIGHTS AND RESPONSIBILITIES	66	PROGRAM COSTS AND PAYMENT	78		
Student Conduct	66	Bachelor's Program Cost	78		
Student Responsibilities	67	Master's Program Cost	79		
Faculty Responsibilities	67	Graduate Certificate Program Cost	79		
Termination of Student Enrollment Agreement	67	Explanation of Regions	80		
Student Complaints and Grievances	68	Fees	80		
UNIVERSITY RIGHTS & RESPONSIBILITIES	70	REFUND POLICY	82		
General	70	ECCU BOARD OF DIRECTORS	84		
		ECCU Advisory Council	84		



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.

A handwritten signature in black ink, appearing to read 'Jay Bavisi', with a stylized, flowing script.

Jay Bavisi
Chairman of the Board of EC-Council University

Mission Statement

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

University History

EC-Council University was incorporated in Wyoming in 2003 and licensed by the New Mexico Higher Education Department in 2006. The institution was created to educate and train cyber security professionals. Cyber security involves in-depth knowledge of a wide array of hardware and software systems as well as the skills and techniques to negotiate them. EC-Council, a world leader and creator of cyber-security certifications used throughout the globe, is the parent company of EC-Council University. EC-Council University Chairman of the Board Sanjay Bavisi believes that cyber security professionals must not only have skills and techniques, but they must be educated to step into leadership and managerial roles in their companies, agencies, and organizations. This belief led to the establishment of the Master of Science 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 the students. In a field as narrow and yet far-reaching as cyber security, these values promote and advance the ultimate goal of educating cyber security experts prepared to make the world safer and more secure for everyone. By incorporating these values with our course content and assessment measures, the educational environment becomes a dynamic and multi-dimensional process that empowers our students to become critical and innovative thinkers as well as, research-oriented problem solvers who embody high ethical standards, leadership skills, and an understanding of the global impact of their work.

Licensure

EC-Council University is licensed by the New Mexico Higher Education Department at 2048 Galisteo Street, Santa Fe, New Mexico, USA, 87505-2100, 505-476-8400.

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

ECCU courseware for CIS 300, CIS301, CIS302, CIS303, CIS304, CIS308, CIS401, CIS402, CIS403, CIS404, CIS405, CIS406, CIS407, 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

EC-Council University is accredited by Distance Education Accrediting Commission (DEAC). The Distance Education Accrediting Commission (DEAC) is a private, non-profit organization founded in 1926 that operates as an institutional accreditor of distance education institutions. Accreditation by DEAC covers all distance education activities within an institution and it provides accreditation from the secondary school level through professional doctoral degree-granting institutions.

Address: 1101 17th Street NW, Suite 808 Washington, DC 20036 | Phone: (202) 332-1386 | Website: www.deac.org

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





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) 910-4153

Enrollment &
Advising Specialist

Email: info@eccu.edu

Phone: (505) 922-2886

Office & Finance
Administrator

Email: finance@eccu.edu

Phone: 505-922-2889

Complaints &
Grievances

Email: registrar@eccu.edu

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
- ➔ Online implementation of iLabs for student engagement
- ➔ Promoting cyber security educational programs and webinars at no cost to the public
- ➔ Preparing our students to be socially responsible in Cyber Security leadership roles

Provide a supportive and welcoming environment to a diverse academic community

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

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 1	January 2, 2018	March 26, 2018	Dec. 2, 2017	January 5, 2018	January 5, 2018	March 11, 2018	March 18, 2018
Term 2	April 2, 2018	June 24, 2018	March 2, 2018	April 6, 2018	April 6, 2018	June 10, 2018	June 17, 2018
Term 3	July 2, 2018	Sep. 23, 2018	June 1, 2018	July 6, 2018	July 6, 2018	Sep. 9, 2018	Sep. 16, 2018
Term 4	October 1, 2018	Dec. 23, 2018	August 31, 2018	October 5, 2018	October 5, 2018	Dec 9, 2018	Dec 16, 2018

2018 HOLIDAYS

New Year's Day	January 1 - Closed	Labor Day	September 3 rd - Closed
Martin Luther King Jr. Day	January 15 th - Closed	Columbus Day	October 8 th - Closed
Presidents Day	February 19 th - Closed	Veterans Day Observed	November 12 th - Closed
Memorial Day	May 28 th - Closed	Thanksgiving Holiday	November 22 nd - 23 rd - Closed
Independence Day	July 4 th - Closed	Winter Break	December 24 th - January 1 st - Closed

2018 COURSE OFFERINGS

Bachelor's Program

Course #	Page #	Course Title for BSCS 2018 - Term 1 Jan. 2, 2018
CIS 301	25	Legal Issues in Information Security
CIS 304	26	Auditing IT Infrastructures for Compliance
CIS 401	27	Strategies in Windows Platforms and Applications
CIS 404	28	*Hacker Techniques, Tools, and Incident Handling (CEH)
CIS 408	29	Wireless and Mobile Device Security
PSY 360	30	Introduction to Social Psychology
COM 340	30	Communications and Technical Writing
CIS 410	30	Capstone

Course #	Page #	Course Title for BSCS 2018 - Term 2 April 2, 2018
CIS 302	25	Managing Risk in Information Systems
CIS 303	26	Security Policies and Implementation Issues
CIS 401	27	Strategies in Windows Platforms and Applications
CIS 405	28	Security Strategies in Web Applications and Social Networking
CIS 406	29	*System Forensics, Investigation, and Response (CHFI)
COM 340	30	Communications and Technical Writing
CIS 410	30	Capstone
BIS 430	31	Ethics for the Business Professional

Course #	Page #	Course Title for BSCS 2018 - Term 3 July 2, 2018
CIS 300	25	Fundamentals of Information Systems Security
CIS 304	26	Auditing IT Infrastructures for Compliance
CIS 402	27	Security Strategies in Linux Platforms and Applications
CIS 403	27	Network Security, Firewalls, and VPNs (CND)
COM 340	30	Communications and Technical Writing
MGT 450	32	Introduction to Project Management
CIS 410	30	Capstone

Course #	Page #	Course Title for BSCS 2018 - Term 4 Oct. 1, 2018
CIS 301	25	Legal Issues in Information Security
CIS 303	26	Security Policies and Implementation Issues
CIS 308	26	Access Control, Authentication, and Public Key Infrastructures
CIS 407	29	Cyber-warfare
COM 340	30	Communications and Technical Writing
ECN 440	31	Principles of Microeconomics
MTH 350	30	Introduction to Statistics
CIS 410	30	Capstone

2018 COURSE OFFERINGS

Master's Program

Course #	Page #	Course Title for MSCS 2018 - Term 1 Jan. 2, 2018
ECCU 501	36	*Ethical Hacking and Countermeasures CEH
ECCU 504	37	Foundations of Organizational Behavior
ECCU 505	38	Introduction to Research and Writing for the IT Practitioner
ECCU 506	38	*Conducting Penetration and Security Tests Disaster Recovery
ECCU 512	41	Beyond Business Continuity: Managing Organizational Change
ECCU 517	43	Cyber Law
ECCU 519	43	Capstone

Course #	Page #	Course Title for MSCS 2018 - Term 3 July 2, 2018
ECCU 501	36	*Ethical Hacking and Countermeasures (CEH)
ECCU 502	37	*Investigating Network Intrusions and Computer Forensics (CHFI)
ECCU 505	38	Introduction to Research and Writing for the IT Practitioner
ECCU 512	41	Beyond Business Continuity: Managing Organizational Change)
ECCU 506	38	*Conducting Penetration and Security Tests Disaster Recovery
ECCU 509	39	Secure Programming
ECCU 514	41	Quantum Leadership
ECCU 519	43	Capstone

Course #	Page #	Course Title for MSCS 2018 - Term 2 April 2, 2018
ECCU 500	36	*Managing Secure Network Systems
ECCU 502	37	*Investigating Network Intrusions & Computer Forensics (CHFI)
ECCU 503	37	*Security Analysis and Vulnerability Assessment (ECSA)
ECCU 504	37	Foundations of Organizational Behavior for the IT Practitioner
ECCU 505	38	Introduction to Research and Writing for the IT Practitioner
ECCU 511	40	Global Business Leadership
ECCU 512	41	Beyond Business Continuity: Managing Organizational Change
ECCU 513	41	*Disaster Recovery (EDRP)
ECCU 519	43	Capstone

Course #	Page #	Course Title for MSCS 2018 - Term 4 Oct. 1, 2018
ECCU 502	37	*Investigating Network Intrusions and Computer Forensics (CHFI)
ECCU 503	37	*Security Analysis and Vulnerability Assessment (ECSA)
ECCU 505	38	Introduction to Research and Writing for the IT Practitioner
ECCU 510	40	Secure Programing (ECSP)
MGMT 502	44	Business Essential
ECCU 519	43	Capstone

* Has a \$50 lab fee

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

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 prior to a decision on admission will be made. A copy of transcripts may be submitted for provisional admission, but for full admission, an official copy must be submitted.

Applicants with a degree from a non-US institution

In addition to the above requirements, applicants with degrees from non-US institutions must provide proof of the US equivalency of your foreign degree. In order to have your degree from a non-US institution evaluated, you must submit unofficial transcripts for all degrees earned to either a National Association of Credential Evaluation Services (NACES) or to National Association for Foreign Student Advisers (NAFSA) evaluator. The transcripts must include a list of all classes completed and grades awarded.

For international transcripts you will need to obtain a NACES or NAFSA evaluation. You will need to contact the University where you earned your degree and request that they send your official transcript and other official documentation as requested by the evaluating agency.

Official transcripts need to be sent to:

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

For NACES: A list of evaluators can be found on the NACES website: <http://www.naces.org/members.html>. The evaluator must send the results of the evaluation directly to ECCU.

For NAFSA: All documents must be sent to ECCU, and the student pays the evaluation fee online.

For both NACES and NAFSA evaluations, all documents written and issued in a foreign language must have a certified English translation attached.

Official 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. All official documents required for full admission must be submitted by the end of the first term. If all required documents are not received by the end of the first term, students will be placed on a registration hold, and may result in the delay in 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. 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 which 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 Provost. Prior to the Provost'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 Provost.

ADMISSION REQUIREMENTS

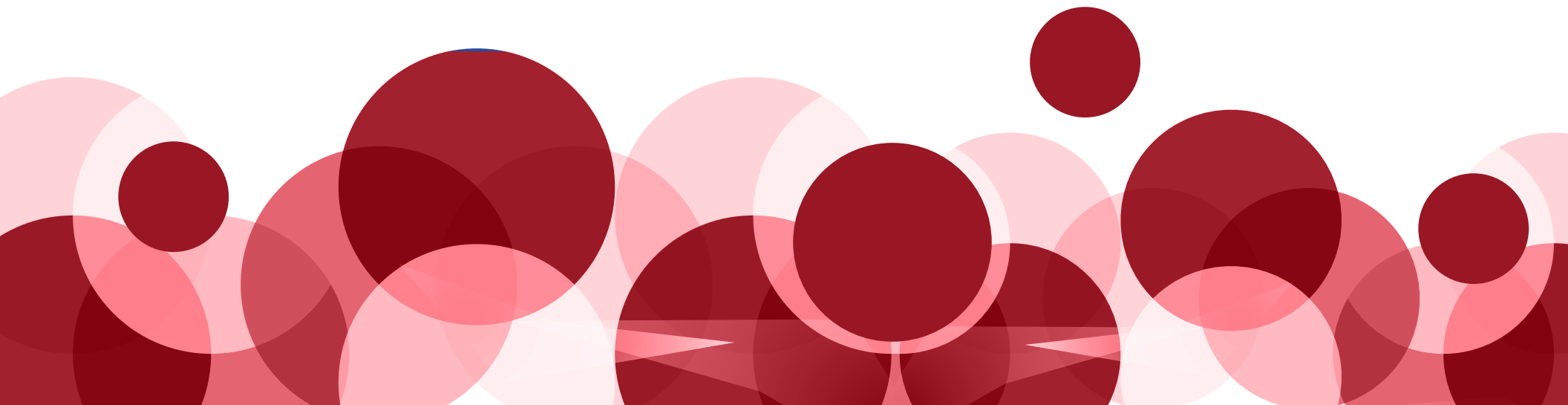
Admission Is Not Guaranteed

Full admission to the university is predicated upon students' submission and the university acceptance of all official documents required for admission, and 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 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 placed on 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 United Kingdom, Canada, Australia, Ireland, New Zealand or Nigeria.
- ➡ If English was the language of instruction at the University where you earned your bachelor's degree then you must provide a letter from the institution stating that English was the language of instruction, and/or you can also request that the NACES or NAFSA evaluator state the language of instruction on the degree evaluation.

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

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








- ➡ 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**
-  **Standard Web browser like Microsoft Internet Explorer (IE), Firefox, or Chrome**
-  **Microsoft Office applications, including, as a minimum: PowerPoint, Word, and Excel**
-  **Adobe PDF reader**
-  **Webcam**
-  **Internet connectivity**
-  **Headphones with microphone (required in some programs)**

STUDENT SERVICES



International Student Admission and Visa Services

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



Scholarship Opportunities

Please see page 71 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 MyECCU. An example student enrollment agreement may be found on the website at: www.eccu.edu



Academic Services

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

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

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)
- ➡ Submit proof of High School Diploma or foreign equivalent
- ➡ Have a cumulative grade point average (CGPA) of 2.0
- ➡ Have completed a college level English and Math class with a grade of C or higher
- ➡ Demonstrate proof of English proficiency (international students only; see 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 students only; see section on English Requirement for International Students)

PROGRAM ADMISSION REQUIREMENTS

Required Admission Documents

The following documents are required for admission:

Bachelor's-Degree-Seeking Students

- ➡ Student Enrollment Agreement
- ➡ Official government ID or passport (international students)
- ➡ 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
- ➡ Proof of completion of 60+ semester credit hours (90+ quarter credit hours) or foreign equivalent
- ➡ Proof of English proficiency (international students only; see section on English Requirement for International Students)
- ➡ Application fee

Master's-Degree-Seeking Students

- ➡ Student Enrollment Agreement
- ➡ Official government ID or passport (international students)
- ➡ Official transcript(s) from the institution where student received 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 section on English Requirement for International Students)
- ➡ Application fee

Military Students

- ➡ 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 cybersecurity academic credits) must have been earned within the last 10 years for consideration. Credits must be from institutions accredited by an agency recognized by the US Secretary of Education and/or the Council for Higher Education Accreditation (CHEA), or an accepted foreign equivalent that is listed in the International Handbook of Universities. The classes must closely correspond with EC-Council University courses and the student must have earned a grade of "B" or higher.

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

Students may receive a maximum of 18 graduate credit hours of transfer credit in the graduate program and 30 credits of transfer credit in addition to the required 60 credits for admission for a total of 90 transfer credit hours in the undergraduate program. Transfer credits are not considered in the calculation of the student's ECCU cumulative GPA.

Prior Learning Portfolio

As a prospective EC-Council University student, you may be awarded appropriate credit for your demonstrated knowledge gained from 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.

Submit all supporting documents to registrar@eccu.edu. Within 5 business days you will be notified of what, if any, credit you will receive and how it will apply to your degree plan.

Certification	Certification Body	Course Equivalent	Degree Program	Credits
Cisco Certified Network Professional (CCNP)	CISCO	CIS 403 & ECCU 500	BSCS & MSCS	3
Cisco Certified Entry Network Technician (CCENT)	CISCO	CIS 403 & ECCU 500	BSCS & MSCS	3
Cisco Certified Network Associate (CCNA)	CISCO	CIS 403 & ECCU 500	BSCS & MSCS	3
Certified Secure Computer User (CSCU)	EC-Council	CIS 300	BSCS	3

TRANSFERRING CREDIT

Certification	Certification Body	Course Equivalent	Degree Program	Credits
Certified Network Defender (CND)	EC-Council	CIS 403 & ECCU 500	BSCS & MSCS	3
Certified Ethical Hacker (CEH)	EC-Council	CIS 404 & ECCU 501	BSCS & MSCS	3
Computer Hacking Forensics Investigator (CHFI)	EC-Council	CIS 406 & ECCU 502	BSCS & MSCS	3
EC-Council Security Analyst (ECSA)	EC-Council	ECCU 503	MSCS	3
Licensed Penetration Tester (LPT)	EC-Council	ECCU 506	MSCS	3
EC-Council Disaster Recovery (EDRP)	EC-Council	ECCU 513	MSCS	3
Certified Chief Information Security Officer (CCISO)	EC-Council		MSCS	3
EC-Council Certified Incident Handler (ECIH)	EC-Council		BSCS & MSCS	3
EC-Council Certified Secure Programmer (ECSP)	EC-Council	ECCU 510	BSCS & MSCS	3
Certified Forensic Computer Examiner (CFCE)	International Association for Computer Information Systems (IACIS)	CIS 406 & ECCU 502	BSCS & MSCS	3
Certified Information Systems Security Professional (CISSP)	International Information Systems Security Certification Consortium (ISC)2	CIS 404 & ECCU 501	BSCS & MSCS	3
Certified Cyber Forensics Professional (CCFP)	International Information Systems Security Certification Consortium (ISC)2	CIS 406 & ECCU 502	BSCS & MSCS	3
Certified Computer Examiner (CCE)	International Society of Forensic Computer Examiners (ISFCE)	CIS 406 & ECCU 502	BSCS & MSCS	3
Microsoft Certified Solutions Associate (MCSA)	Microsoft	CIS 403 & ECCU 500	BSCS & MSCS	3
Microsoft Certified Solutions Expert (MCSE)	Microsoft	CIS 403 & ECCU 500	BSCS & MSCS	3
GIAC Penetration Testing (GPEN)	SANS	CIS 404 & ECCU 501	BSCS & MSCS	3
GIAC Certification Forensics Analyst (GCFA)	SANS	CIS 406 & ECCU 502	BSCS & MSCS	3
Global Information Assurance Certification (GIAC)	SANS	CIS 404 & ECCU 501	BSCS & MSCS	3

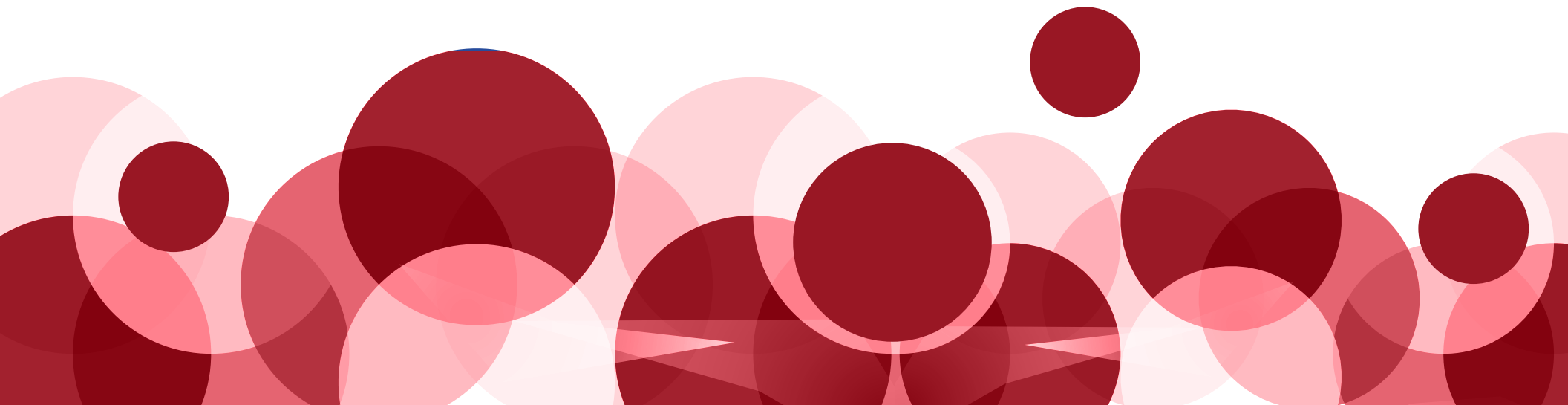
TRANSFERRING CREDIT

Maximum Allowable Transfer Credit

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

Transferability of EC-Council University Credit

Decisions concerning the acceptance of credits or degrees earned at EC-Council University are at the discretion of the receiving institution. Students considering continuing their educations at, or transferring to, another institution must not assume that credits or degrees earned at ECCU will be accepted by the receiving institution. An institution's 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

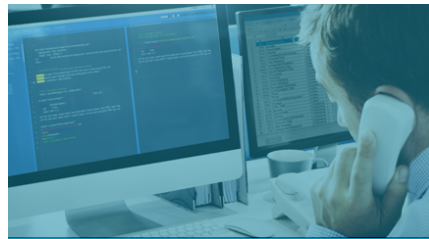
Graduate Programs

- ➡ Master of Science in Cyber Security
- ➡ Graduate Certificate Program

Graduate Certificate Program Selections:



**GRADUATE CERTIFICATE
INFORMATION SECURITY
PROFESSIONAL**



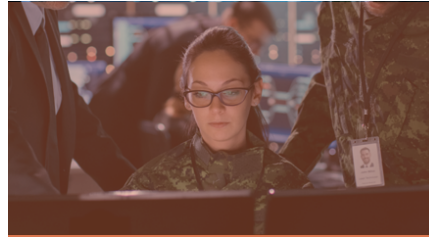
**GRADUATE CERTIFICATE
SECURITY ANALYST**



**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 cyber security applications, tools, and techniques used in today's job work force for careers in Cyber security. It prepares students to obtain knowledge for careers in information technology, and specifically in cyber security. The program features a state of the art virtual labs environment to allow students hands on experience in using the tools of a cyber security professional in a safe, secure online environment. Covering areas dealing with network management, computer security, incident response, and cyber security threat assessment, the program prepares the student for any entry level position in the cyber security field.

BSCS Program Objectives

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

- ➡ 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 cyber security 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 of the summative capstone course
- ➡ All degree requirements must be completed within one and a half times the program length or have a cumulative course completion rate of 67% of course work from the date the student enrolls in the University and begins the program.

BACHELOR OF SCIENCE IN CYBER SECURITY

Bachelor's degree core requirements

All courses are 3 Credit Hours. 45 credits required

CIS 300 - Fundamentals of Information Systems Security pg 26	3 Credits
CIS 301 - Legal Issues in Information Security pg 26	3 Credits
CIS 302 - Managing Risk in Information Systems pg 26	3 Credits
CIS 303 - Security Policies and Implementation Issues pg 27	3 Credits
CIS 304 - Auditing IT Infrastructures for Compliance + pg 27	3 Credits
CIS 308 - Access Control, Authentication, and Public Key Infrastructure + pg 27	3 Credits
CIS 401 - Strategies in Windows Platforms and Applications pg 28	3 Credits
CIS 402 - Security Strategies in Linux Platforms and Applications + pg 28	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 405 - Internet Security: How to Defend Against Attackers on the Web + pg 29	3 Credits
CIS 406 - *System Forensics, Investigation, and Response (CHFI) pg 30	3 Credits
CIS 407 - Cyber-warfare pg 30	3 Credits
CIS 408 - Wireless and Mobile Device Security + pg 30	3 Credits
CIS 410 - Capstone pg 31	3 Credits

Core Courses/Prerequisites:

BIS 430 - Ethics for the Business Professional pg 32	3 Credits
COM 340 - Communications and Technical Writing pg 32	3 Credits
MGT 450 - Introduction to Project Management pg 33	3 Credits

Electives: Select 6 credits from the following courses:

ECN 440 - Principles of Microeconomics pg 32	3 Credits
MTH 350 - Introduction to Statistics pg 31	3 Credits
PSY 360 - Introduction to Social Psychology pg 31	3 Credits

Total credit hours required for the BSCS Program

60 Credits

+ Course has a proctored exam

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

COURSE DESCRIPTIONS

Undergraduate level Courses

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

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

Course Learning Outcomes

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

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

Addresses the area where law and cyber security concerns intersect. cyber security systems and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous cyber security and privacy responses into their daily operations

to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers.

Course Learning Outcomes

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

CIS 302 - Managing Risk in Information Systems (3 Credits)

Provides a comprehensive overview of the SSCP® Risk, Response, and Recovery Domain in addition to providing a thorough overview of cyber security risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk.

Course Learning Outcomes

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

COURSE DESCRIPTIONS

CIS 303 - Security Policies and Implementation (3 Credits)

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

Course Learning Outcomes

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

CIS 304 - Auditing IT Infrastructures for Compliance (3 Credits)

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

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

Course Learning Outcomes

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

CIS 308 - Access Control (3 Credits)

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

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

Course Learning Outcomes

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

COURSE DESCRIPTIONS

- New information on the Identity Theft Enforcement and Restitution Act and the Digital Millennium Copyright Act (DMCA).

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

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

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

Course Learning Outcomes

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

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

Covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion of the risks, threats,

and vulnerabilities associated with Linux as an operating system using current examples and cases. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system. + Course has a proctored exam.

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

Course Learning Outcomes

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

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

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

Upon successful completion of this course, students may take the Certified

COURSE DESCRIPTIONS

Network Defender (CND) certification exam through EC-Council for a discounted price of \$150.

If students wish additional information to assist them to prepare for the certification exam they may purchase an iLab at an additional cost of \$50.00.

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

Course Learning Outcomes

- ➊ New information on Internet Protocol Version 4 (IPv4) with clarification on the difference between IPv6 and IPv4
- ➋ Discusses some of the faults of DNS
- ➌ New information on “Mobile IP” and “Bring Your Own Device”
- ➍ Discusses the use of a sniffer tool or Wireshark
- ➎ Uncovers VPN implementation via cloud application
- ➏ Updated statistical information and industry data

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

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

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 wish additional information to assist them to prepare for the certification exam they may purchase an iLab at an additional cost of \$50.00.

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

Course Learning Outcomes

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

CIS 405 - Internet Security: How to Defend Against Attackers on the Web (3 Credits)

Provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, the book explores the evolutionary changes that have occurred in data processing and computing, personal and business communications, and social interactions and networking on the Internet. It goes on to review all the cyber security risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet. Using examples and exercises, the Second Edition incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications. + Course has a proctored exam

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

COURSE DESCRIPTIONS

Course Learning Outcomes

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

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

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

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.

If students wish additional information to assist them to prepare for the certification exam they may purchase an iLab at an additional cost of \$50.00.

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

Course Learning Outcomes

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

- ➡ Mac Forensics
- ➡ Linux Forensics
- ➡ Mobile Forensics

CIS 407 - Cyber Warfare (3 Credits)

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

Prerequisite: CIS 300 and CIS 301

Course Learning Outcomes

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

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

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

COURSE DESCRIPTIONS

Prerequisite: CIS 300 and CIS 301

Course Learning Outcomes

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

CIS 410 - Capstone Course (3 credits)

This course serves as a comprehensive assessment of knowledge and skills in cyber security systems and cyber security. Activities include research into selected security problems and planning, designing and implementing security solutions for a user organization. Students can enroll in the Capstone after of successful completion of all core degree requirements but must be within 6 credit hours of graduation Students must attainment of a 2.0 cumulative grade point average and have the registrar approval to register in this class.

Course Learning Outcomes

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

PSY 360 - Social Psychology (3 Credits)

Why do individuals behave in a certain manner? How do relationships, people, and society influence such behaviors? The purpose of this course is to introduce you to the field of social psychology, but more specifically to help you understand how others influence our behaviors. This course will provide a general overview of human behavior in a social matrix. The

course will explore topics and concepts such as: social psychology research, the self, prejudice and discrimination, attraction, relationships, aggression, socialization and conformity.

Course Learning Outcomes

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

MTH350 - Introduction to Statistics (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

- 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.

COURSE DESCRIPTIONS

- ➡ Perform hypothesis tests.
- ➡ Think critically about information consumed in daily life and use an understanding of statistics to make good decisions based on that information (statistical literacy).

COM 340 - Communications and Technical Writing (3 Credits)

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

Course Learning Outcomes

- ➡ 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

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

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

ECN 440 - Principles of Microeconomics (3 Credits)

Economics is the study of how a society manages its resources. In most societies, resources are allocated through combined choices of their individual members. Economists study how people make decisions, how they work, what they buy, how much they save, and how they invest those savings. Economists also study how people interact with one another.

Finally, economists analyze forces and trends that affect the economy as a whole, including the growth of income, the fraction of the population that cannot work, and the rate at which prices are rising or falling. This course covers these concepts and more.

COURSE DESCRIPTIONS

Course Learning Outcomes

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

MGT 450 - Introduction to Project Management (3 Credits)

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

Key Features

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

MASTER OF SCIENCE IN CYBER SECURITY

Master of Science in Cyber Security (MSCS) Program Description

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

MSCS Program Objectives

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

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

Master's Degree Graduation Requirements

Each candidate for graduation must meet the following degree requirements.

- ➊ Completion of thirty-six (36) credits of 500 level courses in which the candidate earned a cumulative GPA of 3.0 or better;
- ➋ Satisfactory completion of the summative capstone course;
- ➌ All degree requirements must be completed within one and a half times the program length or have a cumulative course completion rate of 67% of course work from the date the student enrolls in the University and begins the program

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

502 MGMT: Business Essentials + pg 38 3 Credits

ECCU 504: Foundations of Organizational Behavior + pg 39 3 Credits

ECCU 516: Hacker Mind: Profiling the IT Criminal pg 43 3 Credits

ECCU 514: Quantum Leadership pg 43 3 Credits

Core Network Security Course

ECCU 500: *Managing Secure Network Systems (CND) pg 37 3 Credits

ECCU 501: *Ethical Hacking and Countermeasures + (CND) 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:

Specializations cannot be taken until all core requirements have been completed.

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
- Information Assurance (IA) Program Manager
- IT Project Manager
- Application Security Engineer/Manager
- 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
- System Administrator
- Systems Security Analyst
- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Vulnerability Assessment Analyst
- Warning Analyst
- Exploitation Analyst
- All-Source Analyst
- Mission Assessment Specialist
- Target Developer
- Target Network Analyst
- Multi-Disciplined Language Analyst
- All Source-Collection Manager
- 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 Security Officer

MASTER OF SCIENCE IN CYBER SECURITY

Specialization B: Enterprise Security Analyst	Credits
ECCU 520: Advanced Network Defense pg 45	3
ECCU 518: Designing and Implementing Cloud Security pg 44	3
ECCU 510: *Secure Programming pg 41	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 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 522: *Incident Handling and Response (ECIH) pg 46	3
ECCU 513: *Disaster Recovery pg 42	3
ECCU 512: Beyond Business Continuity: Managing Organizational Change pg 42	3

Jobs

- Director/Manager – Business Continuity
- Information Assurance (IA) Program Manager
- IT Project Manager
- Disaster Recovery Analyst/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 523: *Executive Governance and Management (EISM/CCISO) pg 47	3
ECCU 515: Project Management in IT Security pg 43	3

Jobs

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

COURSE DESCRIPTIONS

Graduate Level Courses

ECCU 500 Managing Secure Network Systems (3 credits)

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

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

Course Learning Outcomes

- ➡ Describe fundamental networking concepts, analyze networking protocols and implement established standards to design a robust networking infrastructure.
- ➡ Assess potential vulnerabilities and threats to network infrastructure, predict the implication of network security breaches and analyze the available countermeasures.
- ➡ Examine different network cyber security mechanisms, analyze available security controls and develop strategies to implement and configure these controls.
- ➡ Evaluate the role of network security policies, and develop comprehensive policies that help in protecting network infrastructure.
- ➡ Describe the working of various networking devices, and develop strategies for secure configuration of these devices.
- ➡ Identify security issues with operating systems and network-based applications, analyze the common vulnerabilities and implement best practices to harden networks.
- ➡ Analyze cryptography algorithms and encryption techniques, and design implementation strategies for privacy and security of information.

- ➡ Compare and contrast various network security tools, and make decisions to deploy proper security tools based on evidence, information, and research.
- ➡ Evaluate physical security mechanisms, examine the issues and recommend the countermeasures to safeguard the network infrastructure.
- ➡ Examine the impact of an incident in the network and develop policies, processes and guidelines for incident handling and disaster recovery.

ECCU 501 Ethical Hacking and Countermeasures (3 credits)

This course focuses on how perimeter defenses work, how intruders escalate privileges, and methods of securing systems. Additional topics include intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and virus creation.

Upon successful completion of this course students may take the Certified Ethical Hacker (CEH) certification exam through EC-Council. + Course has a proctored exam

Course Learning Outcomes

- ➡ Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.
- ➡ Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing cyber security of various components of cyber security systems.
- ➡ Compare and contrast different cyber security hacking techniques and analyze the legal implications of hacking.
- ➡ Examine different cyber security vulnerabilities, threats and attacks to information systems and recommend the countermeasures.
- ➡ Analyze cryptography algorithms and encryption techniques, and design

COURSE DESCRIPTIONS

implementation strategies for securing information.

- ➡ Compare and contrast various network security assessment and hacking tools.
- ➡ Assess various network security techniques and tools and implement appropriate level of cyber security controls based on evidence, information, and research.

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

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

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

Course Learning Outcomes

- ➡ Describe computer crime and computer investigation process and develop skills associated to the cyber security professional actively helpful in the field of computer forensics and Incident handling.
- ➡ Acquire, extract, and analyze all the relevant cyber security digital evidence from computing devices using the most appropriate industry-accepted procedures and techniques to investigate computer crime.
- ➡ Consider different perspectives of data acquisition and duplication and develop an organizational strategy on investigating and monitoring the logs that will uphold in the court of law.
- ➡ Understand the structure of file systems and hard disk and recover hidden/deleted files or partitions.

- ➡ Understand various cybersecurity attacks and Internet crimes and use the set of procedures accepted by court of law to investigate Internet crimes.
- ➡ Compare and contrast different forensic tools used in Forensics Investigations.
- ➡ Identify the ethical and legal implications used in the gathering, preserving, documenting, and dispatching of forensic evidence that will be upheld in the court of law.

ECCU 503 Security Analysis and Vulnerability Assessment (3 credits)

This course focuses on testing methods and techniques to effectively identify and mitigate risks to the cyber security of a company's infrastructure. Topics include penetration testing methodologies, test planning and scheduling, information gathering, password cracking penetration testing and security analysis, social engineering penetration testing and security analysis, internal and external penetration testing and security analysis, router penetration testing and security analysis, and reporting and documentation.

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

Prerequisite 501

Course Learning Outcomes

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

COURSE DESCRIPTIONS

ECCU 504 Foundations of Organizational Behavior for the IT Practitioner (3 credits)

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

Course Learning Outcomes

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

ECCU 505 Introduction to Research and Writing for the IT Practitioner (3 credits)

This foundational core course introduces students to basic English writing skills and research methods, including: APA style writing, citing sources, determining when a website is credible, effective communication, outlines, and collaboration. Students will write/present portions of the above in the course in various formats.

Course Learning Outcomes

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

ECCU 506 Conducting Penetration and Security Tests (3 credits)

This course focuses on mastery of the international standard for penetration testing. Topics include customers and legal agreements, penetration testing planning and scheduling, information gathering, external and internal network penetration testing, router penetration testing, firewalls penetration testing, intrusion detection system penetration testing, wireless networks penetration testing; password cracking penetration testing, social engineering penetration testing, PDA and cell phone penetration testing, and penetration testing report and

COURSE DESCRIPTIONS

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

- ➡ Examine various penetration testing mechanisms, and choose suitable set of tests that balance cost and benefits.
- ➡ Examine the penetration testing techniques that perform the intensive cyber security assessments required to effectively identify and mitigate risks to the security of your infrastructure.
- ➡ Demonstrate the compliance of the cyber security system (BS7799, HIPAA etc.) and adopt best practices by conforming to legal and industry regulations.
- ➡ Examine various network security devices, test for vulnerabilities and analyze the reports.
- ➡ Identify vulnerabilities that could be exploited and predict the effectiveness of additional cyber security measures in protecting information resources from attack.
- ➡ Perform internal and external penetration test audits on network infrastructure components and analyze the result.
- ➡ Analyze the techniques involved in gathering sensitive information and choose the best way to find the target company's information.
- ➡ Discover any unauthorized access points and check for any services running on the wireless network.
- ➡ Examine various password cracking techniques, analyze the sensitive information and predict the implications.
- ➡ Examine the post penetration testing actions, analyze the results and present the findings clearly in the final report.

ECCU 507 Linux Networking and Security (3 credits)

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

+ Course has a proctored exam

Prerequisite ECCU 500.

Course Learning Outcomes

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

ECCU 509 Securing Wireless Networks (3 Credits)

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

COURSE DESCRIPTIONS

Course Learning Outcomes

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

ECCU 510 Secure Programming (3 credits)

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

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

Course Learning Outcomes

- ➡ Understand the importance of secure programming and implement a standard set of secure programming practices, policies, and guidelines to develop robust software applications.
- ➡ Compare various application development models and methodologies

and implement a threat modelling approach to balance between usability and security of applications.

- ➡ Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information flow in the applications.
- ➡ Understand the fundamental security concepts used by different programming languages and analyze the usability of different programming constructs in developing secure applications.
- ➡ Identify the common vulnerabilities, threats and attack vectors in different programming languages, assess the implications and determine the appropriate countermeasures.
- ➡ Analyze the working of port scanners and hacking tools and write exploits to assess the application security for common attack vectors based on evidence, information, and research.
- ➡ Understand the security implications of application documentation and error messages and modify default documentation and error message settings so as not to reveal sensitive information.
- ➡ Compare and contrast different application testing and debugging approaches, develop application testing strategy and explore the ways to avoid classic testing mistakes.
- ➡ Examine updates, activation, piracy, and other real time application deployment issues and implement controls for secure data communication between various applications.
- ➡ Compare and contrast different tools that help in developing secure codes and assess the role of these tools in reducing development time and cost thereby adhering to programming ethics.

ECCU 511 Global Business Leadership (3 credits)

This course is designed to provide fundamental skills needed to understand global leadership concepts such as developing technological savvy, appreciating diversity, building partnerships, creating shared vision, maintaining a competitive advantage, integrity and leading for change. This is a study of current and historical leadership theories with emphasis

COURSE DESCRIPTIONS

on viewing the leadership function in the context of global organizational behavior and organizational designs.

Prerequisite ECCU 505.

Course Learning Outcomes

- ➊ Define the 15 dimensions of global leadership
- ➋ Explain the value of diversity in organizations
- ➌ Demonstrate exceptional leadership
- ➍ Evaluate/Analyze a large group of individuals for effectiveness
- ➎ Manage large cyber security teams with ease and confidence
- ➏ 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

- ➊ 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.
- ➋ Determine how individuals and organizations learn from the process
- ➌ Understand that success in all fields of Information technology is underpinned by an ability to understand and manage the "human factor."

- ➍ Compare the value of an organizational design that advances learning to one that inhibits learning.
- ➎ Analyze how individuals react to change and how the manager deals with their reaction.
- ➏ Determine how supervisors serve as change agents and overcome resistance to change.

ECCU 513 Disaster Recovery (3 credits)

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

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

Course Learning Outcomes

- ➊ Understand the various types of disasters and analyze their consequences and effects on organization.
- ➋ Evaluate the need for cyber security disaster recovery and identify the phases involved in the process of recovery.
- ➌ Prepare and implement business continuity plan to ensure the protection of organizational assets and business operations.
- ➍ 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.
- ➎ Analyze the issues related to information system security examine the security mechanism for data backup, role of certification and accreditation authority in securing information systems and identify the technology or services required to recover the data.

COURSE DESCRIPTIONS

- ➊ Understand laws and acts related to disaster recovery that are applicable in various countries and analyze their impact.
- ➋ Assess ethical and legal requirements while undertaking disaster recovery and business continuity services.
- ➌ Understand various virtualization platforms, assess their roles in disaster recovery, and implement these platforms for optimized resource utilization and availability.

ECCU 514 Quantum Leadership (3 credits)

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

Prerequisite: *ECCU 505*

Course Learning Outcomes

- ➊ Develop the role a leader plays in the development and maintenance of the culture.
- ➋ Identify the key issues of the GLOBE Research Leadership project.
- ➌ Design the three levels of culture along with its individual characteristics.
- ➍ Explain the role of individual differences and characteristics in leadership.
- ➎ Examine the function of power and its key role in leadership.
- ➏ Distinguish between transactional and transformational leadership.
- ➐ Explain the leadership practices necessary to implement change.
- ➑ 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 cyber security planning perspective - specifically IT Project Management. Students will learn how to use IT framework to develop an effective IT security project plan. This process will help reinforce IT project management skills while providing the student with a road map for implementing IT security in an organization.

Course Learning Outcomes

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

ECCU 516 The Hacker Mind: Profiling the IT Criminal (3 credits)

Cyber space has increased human communication, connectivity, creativity, capacity and crime by leaps and bounds in the last decade. For all of the positive aspects it offers, it offers as many negative aspects as well. Those negative aspects are explored and developed by everyone from the

COURSE DESCRIPTIONS

high school challenge hacker to the international terrorist. Businesses, governmental agencies, militaries, and organizations of every kind are threatened by the IT criminal. This course will survey the full spectrum of psychological attributes which constitute the profile of the IT criminal.

Prerequisite: *ECCU 505*

Course Learning Outcomes

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

ECCU 517 Cyber Law (3 credits)

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

Prerequisite *ECCU 505*

Course Learning Outcomes

- Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet cyber security.

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

ECCU 518 Special Topics (3 credits)

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

Prerequisites *ECCU 500 and 505.*

Course Learning Outcomes

- The ability to apply knowledge of cloud computing and be able to articulate a migration strategy from legacy open access technologies to cloud technology.
- An ability to analyze a problem, and identify and define the cloud computing requirements appropriate to its solution.
- Students will know the advantages of applying cloud technology to computing applications, communications and information storage.
- An ability to communicate effectively with a range of audiences

COURSE DESCRIPTIONS

- ➡ An ability to analyze the local and global impact of computing on individuals, organizations and society.
- ➡ An ability to use current information security techniques, skills and tools necessary for cloud computing practice.

ECCU 519 Capstone (3 credits)

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

Course Learning Outcomes

- ➡ Perform assessment of the cyber security needs, analyze the internal and external cyber security threats, and determine and implement the methodologies to secure the cyber security systems of an organization.
- ➡ Perform a cyber security audit of a complete information system
- ➡ Identify a cyber security attack, collect necessary evidence in a forensically sound manner and trace the perpetrator of crime.
- ➡ Implement the best and most appropriate strategy for re-meditating the situation
- ➡ In an effective manner, communicate to the staff or business partners (all constituents and stakeholders) the occurrence, ramifications, etc., of that cyber security attack.
- ➡ Create a “protective solution” including auditing and penetration testing of IS to help protect the business or organization from experiencing a similar situation.
- ➡ Effectively manage all pertinent personnel that are impacted by the cyber-attack by designing and implementing standard cyber security policies, procedures and trainings.

- ➡ Identify the common thread to the organizational impact as well as the security impact of successive network innovations.
- ➡ Define a set of useful ideas or “laws of identity” that an IS technician can use to reduce insider threat.

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 the advanced persistent threats.

Prerequisite ECCU 501

Course Learning Outcomes

- ➡ Comprehend 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 identification 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 secure system and network configurations.
- ➡ Comprehend how to establish a secure baseline in deploying machines in a protected state and demonstrate popular attack methods applied by hackers in order 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.

COURSE DESCRIPTIONS

- ➊ 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.
- ➋ Learn 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 common 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.

Prerequisite ECCU 501 and ECCU 502

Course Learning Outcomes

- ➊ Outline the common attacks through Mobile Device Security Hardening and understand what works best for corporate users.
- ➋ Understand how to refine current mobile forensic processes by addressing its unique problems of preserving crucial data and producing valid results.
- ➌ Understand how a Digital or Mobile Forensic Investigator processes cell phones, PDAs, and any other mobile devices that is able to store data and communicate.
- ➍ Learn 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.
- ➎ 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.
- ➏ Compare and contrast various Mobile forensics and analysis Tools

- ➐ Comprehend the concepts of Mobile Reverse Engineering and Outline the skills required for performing it.
- ➑ Learn 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.
- ➒ Investigate the processes involved in Mobile Forensic Acquisitions, Analysis and Reporting of Mobile Device evidence with detailed coverage on some 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

- ➊ Comprehend fundamental skills that are required to handle and respond to the computer security incidents in an information system.
- ➋ Understand various types of incidents, risk assessment methodologies, and check for precautions.
- ➌ Learn various principles, processes and techniques for detecting and responding to security threats/breaches.
- ➍ Learn how to handle incidents, conduct assessments and comprehend various incidents like malicious code, network attacks and insider attacks.

- ➊ Understand the role of computer forensics in handling and responding to the incidents.
- ➋ Learn about incident response teams, incident reporting methods, and incident recovery techniques.
- ➌ Understand various laws and policies related to incident handling and learn how to liaison with legal 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

- ➊ Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.
- ➋ Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies.
- ➌ 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.
- ➍ 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.

- ➎ 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 organization's objectives
- ➏ Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
- ➐ Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls, and design an access control plan.
- ➑ Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks.
- ➒ Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives.
- ➓ Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis.

ECCU 524 Designing and Implementing Cloud Security (3 credits)

This course focuses 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

- ➊ Understand fundamentals of cloud computing, cloud services, cloud computing service models, deployment models, and security considerations of cloud computing.

COURSE DESCRIPTIONS

- ➡ Comprehend secure cloud computing environment design
- ➡ Understand 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
- ➡ Comprehend various types of attacks on a cloud environment and techniques to overcome attacks.
- ➡ Learn about various configuration management techniques, risk assessment methodologies, penetration testing, and Intrusion detection systems (IDS) for a secured cloud environment.
- ➡ Understand the compliance to established industry standards, acts, and laws including PCI-DSS, HIPAA, Sarbanes-Oxley, and Data Protection Act.
- ➡ Discuss the legal issues such cloud computing contracts, vendor transitioning, auditing cloud data, maintaining privacy and confidentiality, geographic jurisdiction, limitations on vendor liability, and taxation challenges.
- ➡ Comprehend Mobile Cloud Computing (MCC) and discuss best practices for secured mobile cloud access.
- ➡ Describe each of the common legal and political issues among nations that affects international business: quotas, tariffs, subsidies, and business practice laws, etc.
- ➡ Demonstrate how companies with different business strategies are best served by having different operations capabilities.
- ➡ Evaluate leadership decision making by discussing rational and behavioral perspectives.
- ➡ Identify the 5 “forces” that constitute the external marketing environment and influence its organizational goals.
- ➡ Aside from the impact of Information Technology has on the business world, identify the threats and risks IT cyber security poses for businesses.
- ➡ Discuss some of the institutions and activities in international banking structures and global finance.

MGMT 502: Business Essentials (3 credits)

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

Course Learning Outcomes

- ➡ Explain the importance of the economic environment to business and analyze the factors used to evaluate the performance of an economic environment.

GRADUATE CERTIFICATE PROGRAM

This is a graduate-level academic program offering specialty areas of study in the cyber-security 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 cyber-security field. The program is targeted towards students wanting to advance in their career 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.

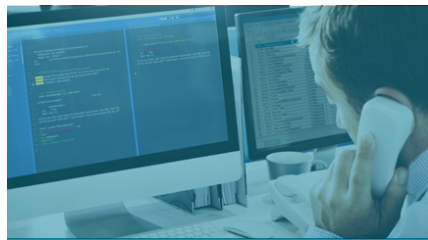
There are six EC-Council University Graduate Certificates: Information Security Professional, Security Analyst, Enterprise Security Architect, Digital Forensics, Incident Management and Business Continuity, and Executive Leadership in Cyber Security. Please see the specific course requirements for each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



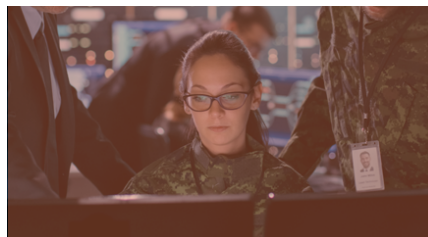
**GRADUATE CERTIFICATE
SECURITY ANALYST**



**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 Cyber Security Professional, as well as basic system security testing and hardening of a target system. This certificate encompasses for the appropriate education and training for an employee in such a position.

II. ECCU Graduate Certificate – 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

Required Courses:

ECCU 510 Secure Programming	3 Credits
ECCU 518 Designing and Implementing Cloud Security (ECSP)	3 Credits
ECCU 520 Advanced Network Defense (prerequisite ECCU 501 (CEH), ECCU 502 (CHFI))	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.

GRADUATE CERTIFICATE PROGRAM

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

ECCU 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 (CCISO/EISM) (prerequisite ECCU 501 (CEH))	3 Credits

Total credit hours

15 Credits

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

TESTING FOR EC-COUNCIL CERTIFICATIONS

Many 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 Secure Programmer (ECSP)	ECCU 510 Secure Programming	
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	

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 4 courses per term. Students 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 or have a cumulative course completion rate of 67% or course work from the date the student enrolls in the University and begins the program.

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

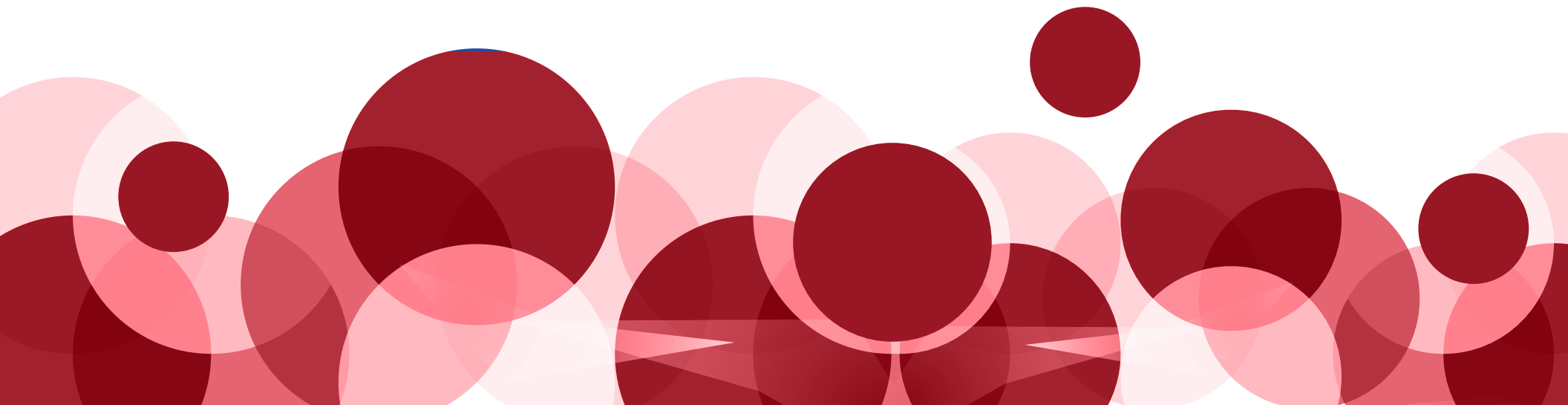
All credits awarded by EC-Council University are semester hour credits and equate with the formula of 45 hours of student work per credit hour per term.

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 three 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 15.

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 or the successful completion of 67% of courses attempted.

Attendance and Participation:

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

Failure to participate in a given weeks 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.

ACADEMIC POLICIES AND GUIDELINES

Leave of Absence:

A leave of absence (LOA) is an interruption in a student's pursuit of degree at EC-Council University. A LOA could be a minimum of one term, or at most, 4 consecutive terms. LOA's will not exceed 2 granted requests.

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

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

Satisfactory Academic Progress

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

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 of assignments, and are expected to maintain the following minimum grade point averages and percentage of credit completion.

- ❶ 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).
- ❷ 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 POLICIES AND GUIDELINES

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 major part of this monitoring process is to review student's cumulative GPA (CGPA) every term. Every student admitted to EC-Council University is expected to maintain continual Satisfactory Academic Progress (SAP).

Failure to maintain SAP in any given term will result in the student being placed on academic probation. Student who do not meet SAP will be referred to the advisor. The advisor will work closely with the student to provide techniques and tools to assist the student to improve their GPA.

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 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 continually make Satisfactory Academic Progress (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).

ACADEMIC POLICIES AND GUIDELINES

Satisfactory Academic Progress Review

Students on Academic Probation (AP) 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 satisfactory academic progress (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 Academic Suspension.

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:

- ➊ The student files an appeal and submits it to the school's Registrar at: registrar@eccu.edu .
- ➋ The Academic Appeals Board (consisting of the Dean, Registrar, and Student Services Manager) review the appeal. Special circumstances were identified to warrant and grant the student's appeal.

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 post- marked or emailed no later than 30 days after the student has received notification of the academic probation or dismissal. After receiving the student's appeal request, the Student Academic Appeals Board (consisting of the Dean, Registrar, and Student Services Manager) 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.

ACADEMIC POLICIES AND GUIDELINES

Cumulative Grade Point Average (CGPA)

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

Percentage of Credit Completion

Percentage of Credit Completion (PCC) shall be calculated by dividing the total number of credit hours for which a student receives a grade of "A", "B", "C", "D" by the total number of credit hours the student has attempted in their program of study. A grade of a "D" is not considered a passing grade for graduate students.

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%).

Examples

- 🕒 If a Master's degree student began taking courses in Term 2-2018 (April 2018) and is taking one course a term, giving them half-time status, they must complete their program by the end of Term 3-2022 (September 2022).
- 🕒 If a Bachelor's degree student began taking courses in Term 1-2018 (January 2018) and is taking 4 courses a term, giving them full-time status, they must complete their degree by the end of Term 4-2019 (December 2019).

ACADEMIC HONESTY POLICY

ECCU Course Policies on Cheating and Plagiarism

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

Cheating	➡ Use of material, information, or study aids not permitted by the faculty
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 such collaboration is not approved by the faculty

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 in the Dean's file of all instances of academic dishonesty for the institution.

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

- ➡ 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 has had a chance to respond, the faculty/staff will determine if academic dishonesty has occurred. If the faculty/staff concludes that academic dishonesty has occurred and has proof, they will report the student's name, the class and assignment, the nature of the academic dishonesty and the proof to the Dean. The type of disciplinary action to be taken will be determined by the student's record of instances identified above and will be applied by the faculty and/or the Dean.

ACADEMIC POLICIES AND GUIDELINES

Citing Sources

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

Original content

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

Timeline

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

Student Identity Verification

- ➊ EC-Council University takes measures to verify the identity of the students who are applying to the university, completing courses, and taking proctored exams.
- ➋ Students access their courses and reference materials through our secure online learning management system, where they are required to enter in their username and password. Each student is responsible for the safeguard of their individual credentials.
- ➌ EC-Council University implements student identity verification in several ways to ensure proper ID.
 - ➊ A Valid Government issued ID is required with admissions application.
 - ➋ Login credentials are required for the online LMS portal.
 - ➌ Proctored exams require a valid photo ID to be presented at time of exam as well as a screen shot of ID.

Remote ProctorNOW Exams

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

GRADING SYSTEM

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

Grade Point Average Calculation

Grade point average (GPA) is calculated by dividing the number of grade points by the number of hours in which a grade of A, B, C, D, or F has been earned. Transfer credits are not included in GPA calculations. All grades count towards credits attempted.

Bachelor's Grading Scale

LETTER GRADE	RANGE OF POINTS	GRADE POINTS
A	90.00-100.00	4.00
B	80.00-89.00	3.00
C	70.00-79.00	2.00
D	60.00-69.00	1.00
F	0.00-59.00	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	90.00-100.00	4.00
B	80.00-89.00	3.00
C	70.00-79.00	2.00
D	60.00-69.00	0.00
F	0.00-59.00	0.00
W	Withdrawal from a course	
AW	Administrative Withdrawal	
I	Incomplete	
IP	In Progress	
R	Retaken Course	

I Incomplete Under some circumstances (i.e. other than lack of effort and study), if all assignments in a course are not completed before its conclusion, the student may request an Incomplete for the course. If the instructor agrees, an "I" will be placed on the student's transcript. The student will have 90 additional days from the end of the term to complete the course and replace the "I" with the assigned letter grade. If, at the end of the normal extension, the student has been unable to complete the course due to extenuating circumstances, s/he may appeal to the Dean for one additional 30-day extension, providing justification as to why they were unable to complete the course. The granting of the Incomplete is at the discretion of the instructor. If the work is not completed before the incomplete expires, the "I" will automatically revert the current earned grade in the course. The student has the right to appeal the instructor's decision to the Dean.

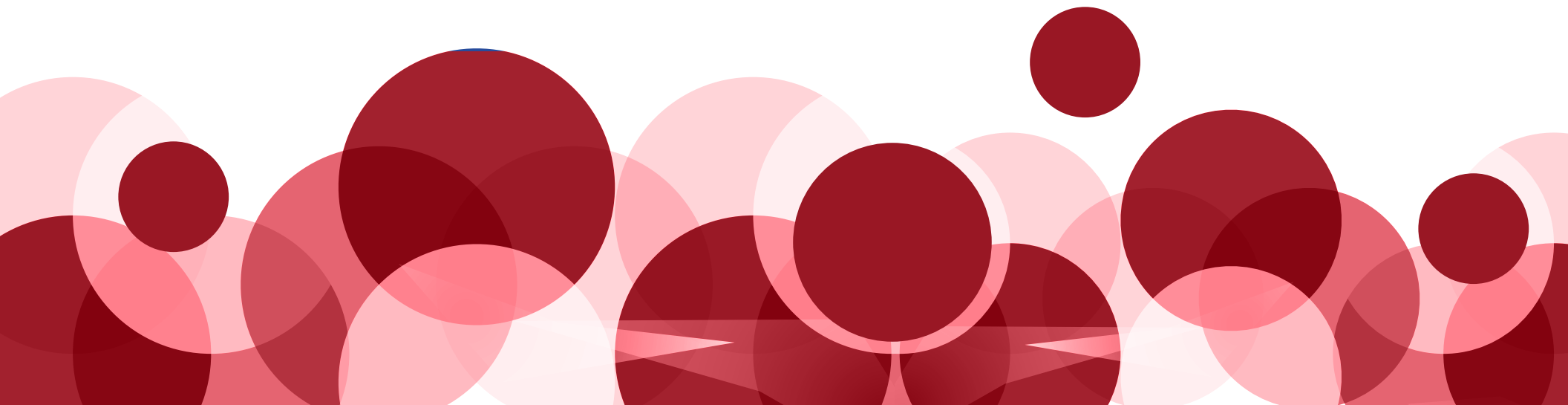
GRADING SYSTEM

IP In Progress applies to currently enrolled courses.

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

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

AW Faculty members or ECCU staff may initiate an Administrative Withdrawal (AW) of a student from a course based on lack of attendance or participation, or lack of connectivity. Please see the description of these items below. Depending on when the AW occurs, the student may be eligible for a refund according to the refund schedule in the refund policy. AW will appear on the student’s transcript and the credits for the course will be added to the credits attempted. If the student is administratively withdrawn from the class because of plagiarism, disciplinary action will occur resulting in the student receiving not an AW but an F on their transcript and the protocol described in the Academic Honesty Policy will be employed. Although students can be dropped for lack of attendance or non-participation, the student should never assume that s/he will be automatically withdrawn for any reason.



GRADING SYSTEM

Lack of Attendance/Participation:

During the first two weeks of class, students who fail to attend class meetings or class related activities or fail to participate without contacting the faculty member and making special arrangements will be administratively withdrawn from class. The faculty member is under no obligation to allow students to make up work they have missed because they failed to attend or participate.

Failure to participate in a given weeks 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

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

The student has completed five classes with the following grades:

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

Total number of grade points **48**

Grade points divided by 15 (total # of hours) = 3.2 GPA

GRADING SYSTEM

Credits

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

Grade Appeal

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

Withdrawal from Program or Course

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

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

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

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

RIGHTS AND RESPONSIBILITIES

Student Conduct

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

A Code of Conduct for the Distance Education Student

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

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

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

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

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:

- ➊ Attend assigned enrolled classes
- ➋ Submit required course work and other assignments required for the program by the prescribed deadlines
- ➌ Behave appropriately within the University environment
- ➍ Be adequately prepared for any activity required as part of the program outside the University, at all times conducting oneself in a proper manner
- ➎ Comply with any professional standards applicable to the program
- ➏ Abide by any special conditions relating to the program set out in the catalog or student enrollment agreement, unless otherwise notified by the University
- ➐ Provide the registrar with an emergency contact name and details which the University may use at its discretion
- ➑ 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:

- ➊ Students have access to necessary materials and resources
- ➋ Students know how and when they may contact the faculty member
- ➌ Students are aware of all relevant academic services available to them (particularly the library and information technology services)
- ➍ 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. Action taken against the student in accordance with the University's disciplinary procedures

RIGHTS AND RESPONSIBILITIES

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

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

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

Step 1

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

Step 2

If the student is dissatisfied or feels unable to confront the individual who is directly responsible, the student will need to notify the Dean at: stanley.lopez@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.

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

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

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

UNIVERSITY RIGHTS AND RESPONSIBILITIES

General

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

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

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

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

Third Parties

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

Rights Reserved

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

STUDENT RECORDS/RIGHT OF PRIVACY

Family Educational Rights and Privacy Act (FERPA) of 1974, as Amended. The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their educational records.

- ➡ The right to inspect and review the student's educational records within 45 days of the day the university receives a request for access;
 - ➡ The student's right to request the amendment of their educational records that the student believes are inaccurate or misleading;
 - ➡ The right to consent to disclosures of personally identifiable information contained in the student's educational records, except to the extent that ferpa authorizes disclosures without consent.
1. Students should submit to the Registrar's office written requests that identify the records they wish to inspect. The University official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the University official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
 2. Students may ask the University to amend records they believe are inaccurate or misleading. They should write the University official responsible for the record, clearly identifying the part of the record they want changed and specifying why it is inaccurate or misleading. If the University decides not to amend the record as requested by the student, the University will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.
 3. Exceptions permitting disclosure without consent is to University officials* with legitimate educational interests. Other known person(s) and agencies are:
 - ➡ School officials with legitimate educational interest
 - ➡ Schools to which a student is transferring
 - ➡ Specified officials for audit or evaluation purposes
 - ➡ Appropriate parties in connection with financial aid to a student
 - ➡ Organizations conducting certain studies for or on behalf of the school
 - ➡ Accrediting organizations; a judicial order or lawfully issued subpoena
 - ➡ Appropriate officials in cases of health and safety emergencies.

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

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

RIGHTS AND RESPONSIBILITIES

Directory Information

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

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

Non-Directory Information

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

Electronic Files

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

Access to Records

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

- ➊ Students 18 years of age or older may examine all records in their name. These records are not available to any other person other than appropriate University personnel, unless released by the student. Legal exception is provided to the above regulation, and these exceptions will be explained to any person who requests the information from the Director of Admissions and Registrar.
- ➋ 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.
- ➌ 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.

RIGHTS AND RESPONSIBILITIES

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 20202-4605 Disability

Disability

The University uses the definition of disability set forth in 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:

- ➊ Has a physical or mental impairment which substantially limits one or more major life activities.
- ➋ Has record of such impairment
- ➌ 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. Student Support Manager will contact student to set up an intake appointment via email.
3. Student Support Manager determines appropriate accommodations.
4. Accommodations will begin within 5 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

RIGHTS AND RESPONSIBILITIES

life function. The diagnostic report must document a disability. It is important 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:

- ➊ Verify a disability; the ADA defines a disability as a substantial limitation of a major life function.
- ➋ 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.
- ➌ 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.
- ➍ Be signed by the medical or mental health professional or diagnostician.
- ➎ Be timely and typed/written on professional letterhead stationary.
- ➏ Be given to Student Support Manager who will begin the intake process.

Documentation may include:

- ➊ Letter from doctor
- ➋ ECCU Diagnosis Verification Request Form
- ➌ DSM diagnosis
- ➍ 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 a long lead time, regular mail service may be an alternative.

RIGHTS AND RESPONSIBILITIES

EC-Council University ensures that all students will be treated equally.

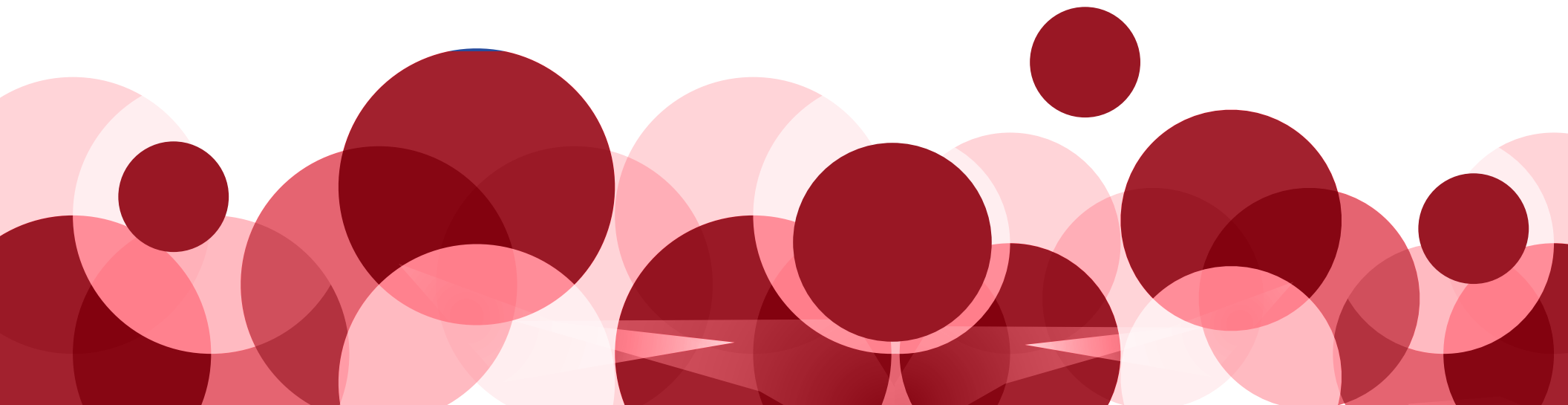
EC-Council University will make available the necessary services for required proctored examinations, however the cost of these services will be borne by the student.

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 needed 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

All online education programs taken as part of an EC-Council programs are covered by the GI Bill®. 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.

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 2 payments are due mid-month (15th) the first and second month of the term. There is no interest charged for this

FINANCIAL ASSISTANCE

payment plan. Good standing on payment plans will ensure continued eligibility for program participation.

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:

- 🔗 The Cybersecurity Ambassador Scholarship
- 🔗 The President's Choice Scholarship for Women
- 🔗 The Dean's Scholarship
- 🔗 New Mexico Scholarship

For details on current scholarship programs, to apply, or express interest see: <https://www.eccu.edu/scholarship/>

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, applied based on the geographical region, of the student plus required fees. To be considered full-time in the Bachelor of Science in Cyber Security program students must be enrolled and complete 12 credits per term.

Additional cost 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.

Region 1	Region 2	Region 3
\$465 Per Credit Hour	\$396 Per Credit Hour	\$330 Per Credit Hour
Application Fee: \$35	Application Fee: \$35	Application Fee: \$35
Technology Fee: \$50 per term	Technology Fee: \$50 per term	Technology Fee: \$50 per term
iLabs Fee: \$50 per certification course	iLabs Fee: \$50 per certification course	iLabs Fee: \$50 per certification course
Graduation Fee: \$150	Graduation Fee: \$150	Graduation Fee: \$150
Transcript fee: \$10+shipping**	Transcript fee: \$10+shipping**	Transcript fee: \$10+shipping**
Transcript w/Apostille: \$20+shipping**	Transcript w/Apostille: \$20+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 6 credits (2 courses) per term for the Master of Science in Cyber Security program or Graduate Certificate program..

Additional cost 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.

Region 1	Region 2	Region 3
\$540 Per Credit Hour	\$473 Per Credit Hour	\$405 Per Credit Hour
Application Fee: \$65	Application Fee: \$65	Application Fee: \$65
Technology Fee: \$50 per term	Technology Fee: \$50 per term	Technology Fee: \$50 per term
Graduation Fee: \$150	Graduation Fee: \$150	Graduation Fee: \$150
iLab Fees: \$50 per certification course	iLabs Fee: \$50 per certification course	iLabs Fee: \$50 per certification course
Transcript fee: \$10+shipping**	Transcript fee: \$10+shipping**	Transcript fee: \$10+shipping**
Transcript w/Apostille: \$20+shipping**	Transcript w/Apostille: \$20+shipping**	Transcript w/Apostille: \$20+shipping**
Specialization: Security Analyst Exam Fee: \$800 iLab Fee: \$200	Specialization: Security Analyst Exam Fee: \$800 iLab Fee: \$200	Specialization: Security Analyst Exam Fee: \$800 iLab Fee: \$200
Specialization: Executive Leadership in Information Assurance Exam Fee: \$999	Specialization: Executive Leadership in Information Assurance 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

Explanation of Regions

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

Region 1: Australia, Austria, Bahrain, Belgium, Canada, Denmark, Finland, France, Germany, Hong Kong, Ireland, Japan, Kuwait, Netherlands, Norway, Oman, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, United Arab Emirates, United Kingdom, and United States.

Region 2: Bahamas, Czech Republic, Chile, Croatia, Estonia, Greece, Hungary, Israel, Italy, Latvia, Lithuania, Malaysia, New Zealand, Panama, Poland, Portugal, Puerto Rico, Romania, Slovenia, Slovakia, South Korean, Spain, Turkey and Uruguay.

Region 3: All of Africa, Argentina, Barbados, Bolivia, Brazil, Bulgaria, Cambodia, Cameroon, China, Colombia, Costa Rica, Egypt, Ecuador, Guatemala, Honduras, India, Indonesia, Jamaica, Jordan, Libya, Mexico, Morocco, Nicaragua, Pakistan, Paraguay, Peru, Philippines, Serbia, South Africa, Thailand, Uganda, Ukraine, Venezuela, and Vietnam.

Fees

Application Fee

There is a \$35 application fee for undergraduate students and a \$65 application fee for graduate (Master's and Graduate Certificate) 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.

Tuition (Course Fee/ credit hour)

🕒 Master's and Graduate Certificate Program: Region 1- \$540/ credit hour; Region 2- \$473/ credit hour; Region 3- \$405/ credit hour

🕒 Bachelor's Program: Region 1- \$465/ credit hour; Region 2- \$396/ credit hour; Region 3- \$330/ credit hour

Lab Fee \$50 (Course Fee) ECCU 500, ECCU 501, ECCU 502, ECCU 503, ECCU 506, ECCU 510, ECCU 513, ECCU 519, ECCU 522, and ECCU 523.

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

PROGRAM COSTS AND PAYMENT

Remote Proctor Now Exams

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.

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.

Technology Fee

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

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.

Tuition costs are payable in USD.

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



REFUND POLICY

Cancellation of Enrollment Agreement

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

Five day cooling off period

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.

After the five day cooling off period

Following the cooling off period, but prior to the beginning of the term, a student may withdraw from enrollment, by notifying the Registrar in a documented manner (mail, e-mail or fax), and ECCU shall be entitled to retain up to \$100 or five percent in tuition or fees, whichever is less. Tuition refunds are calculated on a per class basis. Percentage of tuition refunded to the student minus the registration fee and application fee, which are non-refundable are based on the following schedule.

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

Graduate Certificate programs (non-traditional) are subject to the above policy.

Upon request by a student or by department, ECCU shall provide an accounting for such amounts retained under this standard within five working days.

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

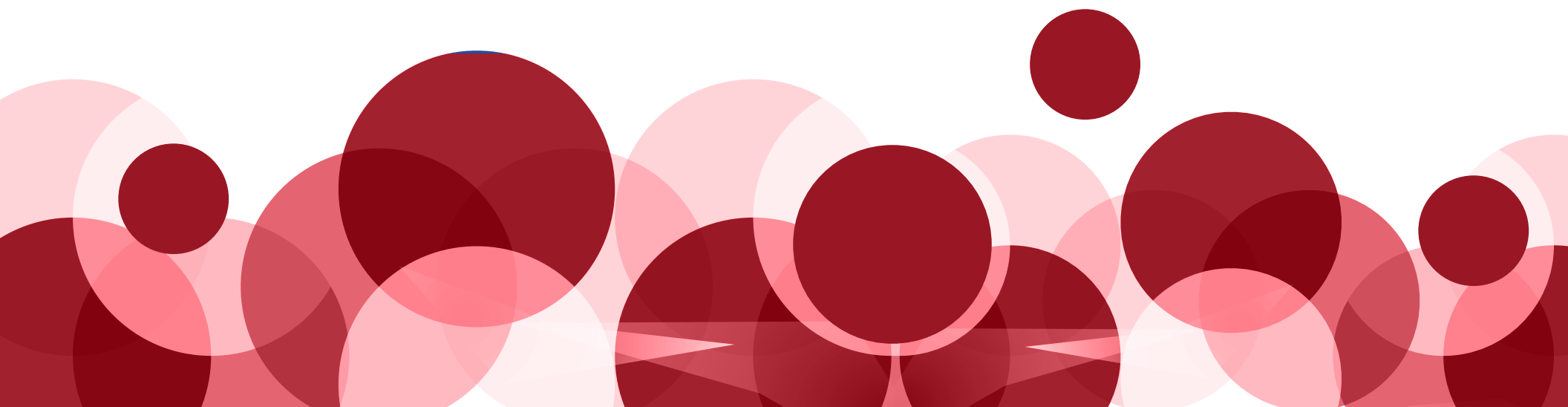
REFUND POLICY

Examples (in USD):

- ➊ Bob began class in the Bachelor's program and paid Region 1 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"
- ➋ Sally returned her Student Enrollment Agreement for the Master's program and paid Region 1 tuition for a 3-credit class with a lab fee, totaling \$1,735. The day before classes began she withdrew from the class. Prior to the beginning of class during a student's first term, students receive a refund of the tuition less the \$65 application fee. Sally received a refund of \$1,670.
- ➌ Mohamed returned his Student Enrollment Agreement for the Bachelor of Science in Cyber Security program, paying Region 3 tuition for a 3-credit class with a lab fee, totaling \$1,040. During the third week, he withdrew from the class. In week 3 of class during a student's first term, students will receive a refund of 60%, less the application fee per the Refund Policy. Mohammed will receive a refund of \$624.
- ➍ Lakshmi was in her second term of classes in the Master of Science in Cyber Security program. She paid Region 2 tuition for a 3-credit class with a lab fee, totaling \$1,469. During the second week of class, she withdrew from the class due to work issues. In week 2 students receive a refund of 70% of the tuition and the lab fee. Lakshmi received a refund of \$1,028.30.

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 Enrollment and Student Services Manager.



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.



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.



Allan Berg

Master of Education, The American University; Bachelor of Science, Towson State University



David Oxenhandler

University of Massachusetts - Master of Business Administration. University of Connecticut - Bachelor of Science - Business



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.

EC-Council University Advisory Council



Stephen Miller

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



Charline Nixon

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 University

EC-COUNCIL UNIVERSITY STAFF



Stanley Lopez, Ph.D.

Dean

- ➔ Doctor of Philosophy in Curriculum & Instruction / Bilingual Education, New Mexico State University
- ➔ Master of Arts in Education Administration and Bilingual Education, New Mexico State University
- ➔ Bachelor of Arts in Spanish / Education, Western New Mexico University



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.



David Valdez

Recruiting and Outreach Specialist

- ➔ Bachelor of Science in Cyber Security, EC-Council University
- ➔ Associate of Arts in Advertising and Marketing, The Art Center Design College
- ➔ Served in the United States Army for 11 years.



Genevieve Buskirk, M.A.

Registrar and Student Services Manager

- ➔ Master of Arts in Sociology, New Mexico State University;
- ➔ Bachelor of Arts in Sociology, New Mexico State University
- ➔ Worked at New Mexico State University Graduate School (Domestic and International Admissions), Dona Ana Community College (High School Recruiting and Admissions), and Brown Mackie College (Registrar).



Kathy Liebhaber

Finance and Office Administrator

- ➔ Worked in Administration as Administrative and Executive Assistant in the Casino and Hospitality industries for 20+ years.
- ➔ Worked in Accounts Payables and Receivables in the Oil & Gas Industry for 7 years.
- ➔ Full Charge Bookkeeper for 2 Burger King Stores for 3 years.

FACULTY



Dominic Boamah, Ph.D.

Adjunct Faculty

Doctor of Philosophy degree (Ph.D.) with emphasis on Information Technology Management, Capella University, Master of Science degree in Information Systems, University of Jyväskylä, Finland



Yuri Diogenes, MS

Adjunct Faculty

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



Matthew Vogel, MS

Adjunct Faculty

Associate of Arts in General Studies, City Colleges, Bachelor of Arts in Information Systems Management, University of Maryland, Masters of Science in Management Information Systems, University of Phoenix



Sandro Tuccinardi, J.D.

Adjunct Faculty

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



Arnold Webster, MS

Adjunct Faculty

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



Yakov Goldberg, MS

Adjunct Faculty

Bachelor of Science, ITT Technical Institute; Master of Science, Capella University



Johnny Justice

Adjunct Faculty

Master of Science, Computer Science Education, Nova Southeastern University; Bachelor of Science, Information Technology Management, American Military University.



Georgia Brown, MS

Adjunct Faculty

Master of Science in Information Technology, Strayer University; Bachelor of Science in Computer Information Systems, Excelsior College.



Linda Walters, MS

Adjunct Faculty

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

FACULTY



Danielle Babb, Ph.D.
Adjunct Faculty

PhD 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
Adjunct Faculty

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



David Moured, Ph.D.
Adjunct Faculty

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



Brian Kirkpatrick, J.D.
Adjunct Faculty

Juris Doctor, Texas A&M University; Master of Arts in Applied Economics, Southern Methodist University; Bachelor of Science in Economics, Texas A&M University



Warren Mack, Ph.D.
Adjunct Faculty

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



Timothy Hill
Adjunct Faculty

Doctor of Business Administration (ABD), California Southern University; Master of Business Administration Strategic Leadership, Amberton University; Master of Science, Information Assurance, University of Maryland University College



“Elle” Ligon
Adjunct Faculty

Master of Science, Business Continuity, Security & Risk Management, Boston University; Bachelor of Information Technology, Concentration in Network Administration, Information Technology, American Continental University.



Kyle Conley
Adjunct Faculty

Master of Science, Information Security and Assurance, Western Governors University; Bachelor of Science, Information Systems Security, American Military University.



Willie Session, Ph.D.
Adjunct Faculty

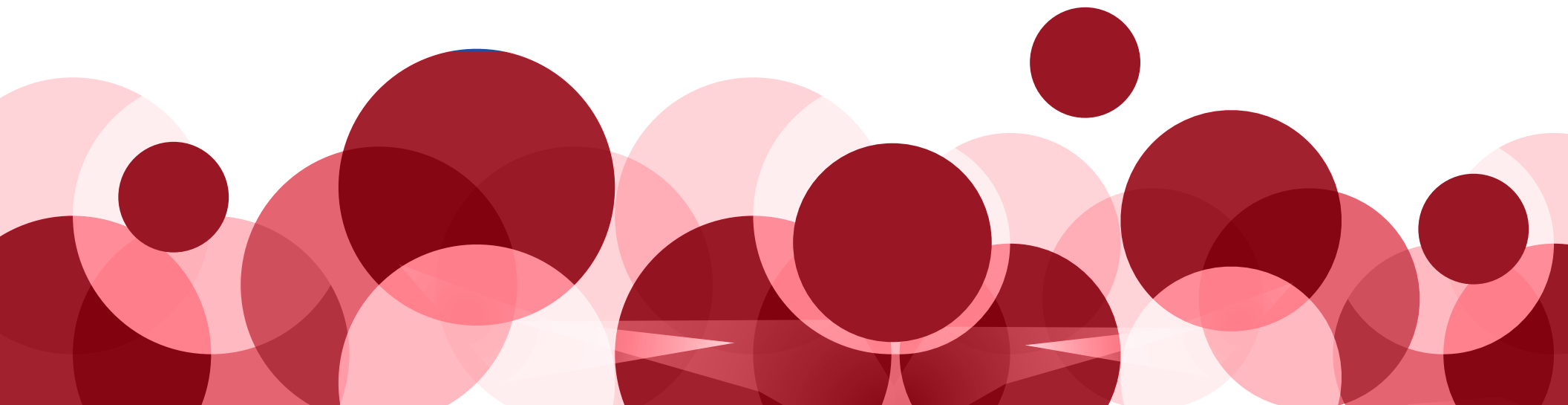
Doctor of Philosophy: Public Policy and Administration, Walden University; Master Business Administration, National University; Bachelor of Science, Southern Illinois University

Copyright

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

The Catalog

This catalog articulates the regulations, policies, programs and procedures for the University and applies to students enrolled between July 1, 2018 and December 31, 2018. Students inactive (not enrolled) for one calendar year must be readmitted and will move forward to the catalog current at the time of their readmission. The catalog is not to be construed as a contract between the student and the University. Not all of the images contained in this catalog are ECCU faculty, staff or students, but they represent the wide diversity of the faculty, staff and students at ECCU. The ECCU Student Enrollment Agreement includes the terms and conditions of attendance at the University. The University reserves the right to change/edit the contents of the catalog as it deems appropriate at any time by means of producing a catalog addendum.



EC-COUNCIL UNIVERSITY

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



info@eccu.edu



www.eccu.edu



1-505-922-2889



1-505-856-8267