

Master of Science in Cybersecurity Studies

This Master of Science in Cybersecurity Studies takes a broad, multi-disciplinary approach to preventing and responding to large-scale cyber threats and cyber attacks. The first half of this program provides you with a foundation in network security, information assurance, cybercrime, and digital forensics. The second half of this program focuses on the issues, policies, practices, and perspectives of various sectors, critical infrastructures, agencies, and disciplines, such as national security, intelligence, criminal justice, and emergency management. Cyber threats can have an adverse effect on public confidence, stock markets, economic sectors, and other critical infrastructures.

This program has specific admission requirements.

Degree Program Objectives

In addition to the institutional and degree level learning objectives, graduates of this program are expected to achieve these learning outcomes:

- Analyze the national cyber threat landscape and cybersecurity challenges from both external entities and domestic sources.
- Examine the legal, social, regulatory, ethical, and technical issues related to securing information systems and national critical infrastructures.
- Compare and contrast the interdisciplinary policies, practices, perspectives and products required to address the cyber threats to our information systems and critical infrastructures.
- Appraise the methodologies for performing vulnerability assessment, risk mitigation, auditing, and certification of information systems and critical infrastructures.
- Categorize the cybersecurity related roles, responsibilities, and policies for managers of critical infrastructures, national security, corporate security, criminal justice, and intelligence/counter intelligence.

Programmatic Admission Requirements

For this program, you must provide an official transcript of your previously completed bachelor's or master's degree and have ONE of the following:

- Associate or bachelor's degree in information technology or a related field (ex: computer science, information systems, database development, etc.)

- 2 years of work experience in the specific sub-field for this degree
- Completion of one of our undergraduate IT certificates
- Completion of 6 credits in IT-related courses
- Completion of an IT-related minor or concentration during your undergraduate program
- Certifications in at least one of the below:
 - a. CompTIA Security+® (2010 to present recommended)
 - b. CompTIA Network+® (2010 to present recommended)
 - c. CompTIA A+® (2010 to present recommended)
 - d. CompTIA Project+® (2010 to present recommended)
 - e. CISSP® certification (valid up until the expiration date)
 - f. SSCP®
 - g. EC-Council Ethical Hacking
 - h. Cisco CCNA® Security
 - i. A valid and current Project Management Professional certification from the Project Management Institute

CompTIA Security+®, CompTIA Network+®, CompTIA A+®, and CompTIA Project+® are all registered trademarks of the Computer Technology Industry Association, Inc.

CISSP® and SSCP® are registered trademarks of International Information Systems Security Certification Consortium, Inc.

CCNA® is a registered trademark of Cisco Technology, Inc.

Notes:

- If the IT-specific requirements are not noted in the official bachelor's or master's transcript, you must provide official copies of your undergraduate transcripts that show the appropriate coursework.
- The verification of the 2-years work experience needs to be sent to the university via formal resume/CV.
- Preadmission courses completed at the undergraduate level must be graded C or better; B or better at the graduate level.

Please visit our AMU (<https://www.amu.apus.edu/admissions/graduate-requirements.html>) or APU (<https://www.apu.apus.edu/admissions/graduate-requirements.html>) graduate admission page for more information on institutional admission requirements.

Need help?

If you have questions regarding a program's admission requirements, please contact an admissions representative at 877-755-2787 or info@apus.edu.

Degree at a Glance

Code	Title	Semester Hours
	Core Requirements	33
	Final Program Requirements	3
	Total Semester Hours	36

Degree Program Requirements

Core Requirements (33 semester hours)

Code	Title	Semester Hours
NSEC506	Cyber Policy and Practice in National Security ¹	3
ITCC500	Research Methods in Information Systems and Technology	3
EDMG600	Emergency Management Perspectives on Cybersecurity	3
HLSS505	Security Risk Management	3
INTL647	Cyber Intelligence	3
ISSC621	Computer Forensics	3
ISSC630	Advanced Cybercrime Analysis	3
ISSC641	Telecommunications and Network Security	3
ISSC642	Intrusion Detection and Incident Handling	3
ISSC660	Information Assurance	3
LSTD517	Law, Ethics and Cybersecurity	3
	Total Semester Hours	33

¹ Required as the first course in the program but may be taken concurrently with another course.

Final Program Requirements (3 semester hours)

Code	Title	Semester Hours
	Select 1 course from the following:	3
ISSC698	Cybersecurity Studies: Capstone Practical ¹	
ISSC699	Cybersecurity Studies Capstone ¹	
	Total Semester Hours	3

¹ This course may not be taken until all other courses are completed and student has a 3.0 GPA