Graduate Certificate - Cybercrime

The graduate certificate in Cybercrime examines the selection and use of digital forensics tools, techniques, and methods used to detect and verify cyber terrorism, cyber warfare, cyberstalking, and cyberbullying. The global reach of the Internet, the low cost of online activity, and the relative anonymity of users has contributed to a steady increase in cybercrime. Talented and trained professionals are needed to combat the effects of this rise in computer-related malice. This certificate program is intended for graduate students who seek to heighten their knowledge of cybercrime without committing to an academic degree program.

This program has specific admission requirements.

Certificate Objectives

Upon successful completion of this certificate, the student will be able to:

- Analyze the domains of knowledge, strategies, countermeasures, and challenges in the areas of cyber terrorism, cyber war, cyber stalking, and cyber bullying.
- Examine the phases, processes, and challenges of cybercrime investigations.
- Appraise the technical, legal, economic, and societal issues related to cybercrime.
- Evaluate the principles, practices, tools, techniques, and procedures to process cybercrime scenes.
- Appraise the legal and regulatory compliance requirements in investigating and prosecuting cybercrime.

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 certificate - to be documented in your resume or your Joint Services Transcript (JST) and DD214
- Completion of one of our undergraduate IT certificates
- Completion of 6 upper-level (300-400) undergraduate credits in IT-related courses
- Completion of an IT-related minor or concentration during your undergraduate program
- Certification from CompTIA A+ (2010 – Present) or a combination of the following (must have two) CompTIA Network +, CompTIA Project +, CompTIA Security+ (all 2010-Present)
- A valid and current Project Management Professional certification from the Project Management Institute
- Completion of CISSP certification (valid up until the expiration date)

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 from your current/previous employer on company letterhead.
- Pre-admission courses completed at the undergraduate level must be graded C or higher; B or higher 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.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC621	Computer Forensics	3
ISSC630	Advanced Cybercrime Analysis	3
ISSC631	Cyber Ethics: Privacy and Intellectual Property	3
ISSC642	Intrusion Detection and Incident Handling	3
ISSC650	Advanced Digital Forensics	3
ISSC651	Advanced eDiscovery	3
Total Semester Hours		18