

Graduate Certificate - Information Systems Security

The graduate certificate in Information Systems Security teaches secure network design, development of security policies and programs, cryptography, business continuity planning, and other skills necessary to protect organizational systems from growing sophisticated attacks. This certificate program is intended for graduate students who seek to heighten their knowledge of information assurance without committing to an academic degree program.

Courseware in this online program aligns with knowledge needed for the Certified Information Systems Security Professional (CISSP) certification, the gold standard certification for international information security.

This program has specific admission requirements.

Certificate Objectives

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

- Compare and contrast the differences between the various network topologies (both physical and logical) and appraise the various types of Security Architecture and Design models.
- Examine the seven-layer OSI networking model and its relation to common protocol stacks and inspect the components of a packet (header, body, CRC, etc.).
- Examine the principles of network security and assess cellular architecture.
- Evaluate the process for securing current and next generation telecommunications networks.
- Examine the principles of intrusion detection and intrusion prevention.
- Differentiate between the different types of cryptographic algorithms.

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 (resume with references required)
- Completion of one of our undergraduate IT certificates (completed in the past 10 years)
- Completion of 6 upper-level (300-400) undergraduate credits in IT-related courses (completed in the past 10 years)
- Completion of an IT-related minor or concentration during your undergraduate program (completed in the past 10 years)
- 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.
- 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.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC621	Computer Forensics	3
ISSC640	Computer Networks and Data Systems	3
ISSC641	Telecommunications and Network Security	3
ISSC642	Intrusion Detection and Incident Handling	3
ISSC660	Information Assurance	3

ISSC680	Information Security Management	3
Total Semester Hours		18