Graduate Certificate: Cyber Defense and Information Assurance

COLLEGE OF SCIENCE AND TECHNOLOGY

Learn more about the graduate certificate in Cyber Defense and Information Assurance.

About the Certificate

The graduate certificate program in Cyber Defense and Information Assurance (CyberDIA) is designed for aspiring technical professionals at all career levels—entry-level, mid-career and senior executives—who want to equip themselves with skills necessary to protect their organization and the nation from increasing cyber threats. The multidisciplinary program design borrows knowledge, skills and expertise from different academic disciplines, including business, computer and information sciences, electrical and computer engineering, and law. The key focus is on a holistic cybersecurity framework, i.e., one that is built around the core principles of preventive, detective and corrective security mechanisms. While the CyberDIA curriculum is technology intensive, focusing on network security and digital forensics, it also bridges the ever-increasing gap between cybersecurity technology and cybersecurity policies. Students take 12 credits of the core curricular classes of the CyberDIA MS program to complete the certificate.

Campus Location: Main

Full-Time/Part-Time Status: The graduate certificate can be completed on a part-time basis. NOTE: International students may not be eligible to apply for a student visa based on admission to the certificate program. Please contact the graduate administrative coordinator for more information.

Non-Matriculated Student Policy: Students can take up to 9 credits on a non-matriculated basis. When they complete 9 credits, they must declare their intention to complete the graduate certificate in Cyber Defense and Information Assurance by completing and submitting the "Non-Degree Seeking Student Request to Exceed 9 Credits of Graduate Coursework for Certificate Program," found in TUportal under the Tools tab within "University Forms."

Admission Requirements and Deadlines

Bachelor's Degree in Discipline/Related Discipline: All applicants must present credentials that are the equivalent of the appropriate baccalaureate degree at Temple University.

Certificate Requirements

Number of Credits Required to Complete the Certificate: 12

Required Courses:

Code	Title	Credit Hours
CIS 5017	Operating Systems and Architecture [1]	3
CIS 5107	Computer Systems Security and Privacy	3
CIS 5405	Introduction to Digital Forensics [2]	3
CIS 5415	Ethical Hacking and Intrusion Forensics [2]	3
Total Credit Hours		**12**

1 With advisor recommendation and approval, students can take CIS 5512 instead.

2 With advisor approval, students who have taken "Introduction to Digital Forensics" and/or "Ethical Hacking and Intrusion Forensics" at the undergraduate level may take an alternate approved course(s) at the master's level.

GPA Required to be Awarded the Certificate: 3.0 minimum

Contacts

Certificate Program Web Address:

https://www.temple.edu/academics/degree-programs/cyber-defense-and-information-assurance-certificate-graduate-st-cdia-grad

Department Information:

Dept. of Computer and Information Sciences
313 Science and Education Research Center
1925 N. 12th Street

Philadelphia, PA 19122-1801
cst.psm@temple.edu
215-204-8450

Submission Address for Application Materials:

https://cst.temple.edu/academics/graduate-programs/apply-now

Department Contacts:

Admissions:
Graduate Administrative Coordinator
cisadmit@temple.edu
215-204-8450

Program Director:
Derek Fisher, MS
derek.fisher@temple.edu
610-858-1971

Graduate Chairperson:
Yan Wang, PhD
y.wang@temple.edu
215-204-1743

Department Chairperson:
Yu Wang, PhD
wangyu@temple.edu
215-204-4187