

# Cyber Defense and Information Assurance PSM

---

## COLLEGE OF SCIENCE AND TECHNOLOGY

Learn more about the Professional Science Master's in Cyber Defense and Information Assurance.

### About the Program

As our physical and digital worlds become more deeply interwoven, a web of interdependence is increasingly fading away the distinction between physical and cyberspace infrastructures. One consequence is that citizens are rendered extremely vulnerable to threats against our cyberinfrastructure by cybercriminals who can inflict crippling blows to pockets of society or even the entire nation. With the dearth of a global information security workforce at a staggering 2.72 million in 2021, the federal government has expressed its support to meet this urgent need.

In designing the Professional Science Master's (PSM) program in Cyber Defense and Information Assurance (CyberDIA), the dynamic and cross-cutting nature of the current and continuously evolving cyberspace and the barrage of ever-increasing and never-ceasing threats it faces were addressed. The program 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 cyberthreats. 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.

**Time Limit for Degree Completion:** 2 years

**Campus Location:** Main

**Full-Time/Part-Time Status:** The degree program can be completed on a full- or part-time basis. Most of the classes are offered in the evenings or on weekends to enable full-time working professionals to be enrolled in the program. International students are required to register as full-time students.

**Interdisciplinary Study:** The CyberDIA curriculum addresses four core knowledge areas:

- Technology (60%)
- Laws, regulations, and governance (15%)
- Policies, procedures, and compliance (15%)
- Leadership and ethics (10%)

**Accreditation:** Temple University is fully accredited by the Middle States Commission on Higher Education.

**Job Prospects:** Official job placement is not offered, but prospects are excellent given the dearth in "Infosec" professionals. Positions include:

- Computer Security Forensic Investigator
- Cybersecurity Systems Engineer
- Information Security Officer
- IT Network Security Penetration Tester
- Security Analyst/Cybersecurity Analyst

**Licensure/Certification:** Successful completion of the CyberDIA PSM program equips students with the necessary knowledge, skills and tools to appear for the following professional certifications:

- Certified Ethical Hacker (CEH) offered by EC-Council
- Certified Information Systems Security Professional (CISSP®) offered by (ISC)<sup>2</sup>
- Computer Hacking Forensic Investigator (CHFI) offered by EC-Council

**Non-Matriculated Student Policy:** Non-matriculated students may enroll in a total of three courses (9 credits) with permission of the instructor and the Department of Computer and Information Sciences.

**Financing Opportunities:** Financial assistance in the form of Research or Teaching Assistantships is not offered.

### Admission Requirements and Deadlines

**Application Deadline:**

*Fall Priority Deadline:* March 1

*Spring Priority Deadline:* October 30

Applications submitted after the priority deadline will be considered for admission on a rolling basis.

*APPLY ONLINE to this graduate program.*

#### **Letters of Reference:**

*Number Required:* 2

*From Whom:* Letters should be obtained from college/university faculty or faculty who are familiar with the applicant's competency. If the applicant has an established career in the field, the applicant's immediate supervisor should provide one of the letters.

**Coursework Required for Admission Consideration:** Applicants should have a strong background in one or more STEM fields: science, technology, engineering and mathematics. The following prerequisites must also be met:

- a course in data structures, such as Temple's CIS 2168, and
- a course in computer architecture, operating systems and networking, such as Temple's CIS 2229.

**Bachelor's Degree in Discipline/Related Discipline:** The CyberDIA PSM program has been designed for recent graduates and professionals who have a bachelor's degree or equivalent in a STEM field.

**Statement of Goals:** In up to 500 words, explain your interest in this specific program and what career goals you have. Describe your work and academic experiences with specific mentions of internships, course projects, or research. Share any other relevant information that you feel should be taken into consideration.

**Transcripts:** Unofficial transcripts are considered at the time of applying. Official transcripts are required when accepting the offer at the time of deposit. Official transcripts can be sent to [cst.gi@temple.edu](mailto:cst.gi@temple.edu)

#### **Standardized Test Scores:**

GRE: Optional

Applicants who earned their baccalaureate degree from an institution where the language of instruction was other than English, with the exception of those who subsequently earned a master's degree at a U.S. institution, must report scores for a standardized test of English that meet these minimums:

- TOEFL iBT: 85
- IELTS Academic: 6.5
- PTE Academic: 58
- Duolingo: 110

**Resume:** Current resume required.

**Interview:** May be required on a case-by-case basis.

**Transfer Credit:** Graduate credits from an accredited institution may be transferred into the CyberDIA PSM program. The credits must be equivalent to coursework offered by the Department of Computer and Information Sciences at Temple University. A grade of "B" or better must have been earned for the credits to transfer. The CyberDIA PSM Steering Committee makes recommendations to the Department Chair for transferring credit on an individual basis. The maximum number of credits a student may transfer is 6.

## **Program Requirements**

#### **General Program Requirements:**

*Number of Credits Required Beyond the Baccalaureate:* 30

*Required Courses:*

| Code                   | Title  | Credit Hours |
|------------------------|--|--------------|
| <b>Core Courses</b>    |  |              |
| CIS 5017               | Operating Systems and Architecture <sup>1</sup>      | 3            |
| CIS 5107               | Computer Systems Security and Privacy                | 3            |
| CIS 5405               | Introduction to Digital Forensics <sup>2</sup>       | 3            |
| CIS 5415               | Ethical Hacking and Intrusion Forensics <sup>2</sup> | 3            |
| <b>Electives</b>       |  | <b>15</b>    |
| <b>Capstone Course</b> |  |              |

|                           |                  |           |
|---------------------------|------------------|-----------|
| CIS 9995                  | Capstone Project | 3         |
| <b>Total Credit Hours</b> |                  | <b>30</b> |

- <sup>1</sup> With advisor recommendation and approval, students can take CIS 5512 instead.
- <sup>2</sup> 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.

**Additional Requirement:** All graduate-level courses must be passed with a "B-" or better.

#### **Culminating Event:**

##### *Capstone Project:*

Each student is given a real security problem. Phase 1 relates to compliance: identifying how the security problem affects the organization and which regulations/standards are to be considered. Phase 2 is the technical piece: identifying network and application vulnerabilities; performing forensics (chain of custody); and documenting findings. In Phase 3, all findings from Phases 1 and 2 are presented to the executive body of the affected organization and the faculty mentor(s).

## **Contacts**

### **Program Web Address:**

<https://www.temple.edu/academics/degree-programs/cyber-defense-and-information-assurance-psm-st-cdia-psm>

### **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:**

#### *Program Director:*

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

#### *Admissions:*

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

#### *Graduate Chairperson:*

Yan Wang, PhD  
y.wang@temple.edu

#### *Department Chairperson:*

Yu Wang, PhD  
wangyu@temple.edu