M.S. Program in Cybersecurity and Privacy (Non-Thesis)- revised Sept 2023

The Computer Science Department at UGA has 7 faculty whose research areas are in cybersecurity and privacy. The Computer Science Department at UGA has established an Institute for Cybersecurity and Privacy (ICSP). The National Security Agency and Department of Homeland Security named the UGA Institute for Cybersecurity and Privacy a National Center of Academic Excellence in Cybersecurity Research.

1) Program Description and Objectives

This MS program will be useful for all students, particularly in the fields of computer science, mathematics, and engineering. The program aims to develop expertise in various aspects of computer security and privacy, such as networking, operating systems, network and systems security, and data and communications privacy.

2) Admission Criteria:

Admissions requirements will align with the current admissions standards set by the Graduate School and the Franklin College of Arts and Sciences. Completed applications will include the UGA graduate application, bachelor's degree from a regionally accredited institution in Computer Science or a related discipline, three letters of recommendation, statement of purpose, a minimum 3.0 GPA, GRE test score and resume. Applicants will need to meet all Graduate School requirements.

Students with insufficient background in Computer Science must first take undergraduate Computer Science courses to remedy any deficiencies, in addition to their graduate program requirements. A sufficient background in Computer Science must include at least the following courses (or equivalents):

- CSCI 1301-1301L, Introduction to Computing and Programming (alternative option CSCI 7010, Computer Programming)
- CSCI 1302, Software Development
- CSCI 1730, Systems Programming
- CSCI 2610, Discrete Mathematics for Computer Science
- CSCI 2670, Introduction to Theory of Computing
- CSCI 2720, Data Structures
- MATH 2200, Analytic Geometry and Calculus
- MATH 2250, Calculus I for Science and Engineering

3) **Curriculum** (This program requires 30 credit hours).

Required Courses (19-20 hours):

- CSCI 6250, Cyber Security (4 hours)
- CSCI 6260, Data Security and Privacy (4 hours)
- CSCI 6730, Operating Systems (4 hours)

- CSCI 6760, Computer Networks (4 hours)
- CSCI 7200, Master's Project (3-4 hours)

Elective Courses (11-12 hours): Choose three courses from:

- CSCI 8240, Software Security and Cyber Forensics (4 hours)
- CSCI 8245, Secure Programming (4 hours)
- CSCI 8250, Advanced Cyber Security (4 hours)
- CSCI 8260, Computer Network Attacks and Defenses (4 hours)
- CSCI 8265, Trustworthy Machine Learning (4 hours)
- CSCI 8960, Privacy-Preserving Data Analysis (4 hours)
- CSCI 8965, Internet of Things Security (4 hours)
- MATH 6450, Cryptology and Computational Number Theory (3 hours)
- CSCI 6270, Introduction to Computer Forensics (4 hours)
- CSEE 8310 Security in Cyber-Physical Systems (3 hours)
- MIST 7775 Cyberthreat Intelligence (3 hours)

To complete the program in Cybersecurity and Privacy (M.S.), students must complete 19-20 hours of required courses in Computer Science, including CSCI 7200 Master's project, spread over two semesters. Students must also complete 10-12 hours of elective coursework related to Cybersecurity and Privacy, and CSCI 3030 or equivalent if they have not already taken a suitable ethics course. Overall, students must complete at least 12 credit hours of graduate-only coursework.

4) PROGRAM OF STUDY

Courses *(list acronym, number, and title)*	**Semester**	**Hours**
Required Courses		
CSCI 6250, Cyber Security	Spring	4
CSCI 6260, Data Security and Privacy	Fall	4
CSCI 6760, Computer Networks	Fall	4
CSCI 6730, Operating Systems	Spring	4
CSCI 7200, Master's Project	Fall	4
CSCI 7200, Master's Project	Spring/Summer	3-4
Elective Courses (Choose three courses)		
CSCI 8240, Software Security and Cyber Forensics	Spring	4
CSCI 8245, Secure Programming	Spring	4
CSCI 8250, Advanced Cyber Security	Spring	4
CSCI 8260, Computer Network Attacks and Defenses	Spring	4
CSCI 8265, Trustworthy Machine Learning	Spring	4
CSCI 8960, Privacy-Preserving Data Analysis	Spring	4
CSCI 8965, Internet of Things Security	Spring	4
CSCI 6270 Introduction to Computer Forensics	Spring	4
MATH 6450 Cryptology and Computational Number Theory	Spring	3

5) Student Learning Outcomes:

a. Students in this program should be able to defend against common cybersecurity and privacy attacks by having knowledge of information security, including secure programming and known practices.

b. Students will be able to use their enhanced and improved hands-on experiences and skills to address various security and privacy issues.

c. Students should be able to make risk assessment to IT design decisions.

Sample Program of Study

	Course Number	Course Title	Hours
First Year Fall	CSCI 6760 CSCI 6720 CSCI 6260	Computer Networks Computer Systems Architecture Data Security and Privacy Total Credit Hours	4 4 4 12
First Year Spring	CSCI 6730 CSCI 6250 CSCI 8260 CSCI 8960	Operating Systems Computer Security Computer Network Attacks and Defenses Privacy-Preserving Data Analysis Total Credit Hours	4 4 4 4 16
Summer	CSCI 7200	Master's Project Total Credit Hours	2-3 2-3
Total			**30**