UNIVERSITY OF ARKANSAS GRANTHAM

Bachelor of Science in Cybersecurity

Category I

Bachelor of Science in Cybersecurity	Credit	CCAF Transfer Credits	Course Credits to be taken at UA Grantham
General Education			
GU100 UAG Engage	1		1
BIO101 Life Science I	4	4	
BIO102 Life Science II	4		4
ECN206 Macroeconomics	3	3	
EN101 English Composition I	3	3	
EN261 Fundamentals of Technical Writing	3	3	
MA100 Quantitative Reasoning	3	3	
HU260 Strategies for Decision Making	3	3	
HU275 Professional Ethics	3	3	
GP210 American Government	3	3	
PS101 Fundamentals of Psychology	3	3	
SO101 Intro to Sociology	3	3	
General Education Requirements	36	31	5
Program Core			
CO201 Conflict and Communications	3	3	
CS192 Programming Essentials	3		3
CS265 Programming in C++	4		4
CS340 Operating Systems	3		3
IS471 Computer Forensics	3		3
CT420 Cyber Phys Systems & Security	4		4
FIN210 Personal Finance	3	3	
IS211 Intro Info Systems Security	3	3	
IS216 Computer Networks	3	3	
IS242 Management Information Systems	3	3	
IS311 Security Operations	3	3	
IS320 Database Applications	3		3
IS336 Systems Analysis and Design	3		3
IS345 Querying in SQL	3	3	
IS355 Risk Management	3		3
IS360 Disaster Recovery	3		3
IS391 Special Topics in Info Systems	1		1
IS411 Network Security	3		3
IS440 Human Decision & Sec Eng	3		3

IS450 Security Trends and Legal Issues	3		3
IS461 Cryptography	3		3
IT330 Linux Administration	3		3
IT340 Cloud Computing Essentials	3		3
IT460 Virtualization	3	3	
IT470 Cloud Computing Security	3		3
MA105 College Algebra	3	3	
MA230 Mathematical Statistics I	3	3	
MA315 Discrete Math	3		3
Program Core Requirements	84	30	54
Total Degree Credit Hours	120	61	59

Updated June 2023

The objective of the Cybersecurity degree program is to provide students with the knowledge and skills to enter the workforce and advance in professional cybersecurity or information security roles. Required coursework builds a foundation and broad base of skills in network protocols, advanced security concepts and operating systems and system architecture. Courses are aligned to the Network+, Security+ and CISSP industry-standard certifications.

Program Educational Objectives

The educational objectives of the program are to produce students who, within a few years of graduation, should be:

- Successfully employed in a position with a security focus in the government or private sectors or be in a graduate program
- Using a variety of security-related skills to improve the security posture of an organization
- Effective as a professional through communication skills, project management skills, ethical conduct, social awareness, and teamwork
- Technically current through continued education, certifications, and professional development

Student Learning Outcomes

- Apply knowledge of computing and mathematics appropriate to the discipline
- Analyze a system and identify and define the security risks and requirements for secure operation
- Design, implement and evaluate a computer-based system, process, component, or program to meet security needs
- Address professional, ethical, legal, security, and social issues and responsibilities
- Communicate effectively with a range of audiences
- Analyze the local and global impact of computing on individuals, organizations, and society
- Recognize the need for and an ability to engage in continuing professional development
- Use current techniques, skills, and tools necessary for computing security practice
- Identify and analyze security risks of an information system
- Develop security and recovery policies appropriate to an information system