THE ASSOCIATE OF APPLIED SCIENCE (A.A.S.)

The Associate of Applied Science Degree is designed for employment purposes, and it should not be assumed that the degree or the courses in the degree can be transferred to another institution. While a few institutions have recently begun to accept some courses in A.A.S. programs, the general rule is that courses in the A.A.S. degree are not accepted in transfer toward bachelor's degrees. Students to whom transfer is important should get assurance in writing in advance from the institution to which they wish to transfer and be aware that they may be required to complete additional lower-division courses to meet specified prerequisite course requirements for their chosen baccalaureate degree program upon Arkansas public university transfer.

ATTENTION STUDENTS: PLEASE SEE CURRENT CATALOG FOR ALL FEES AND CHARGES ASSOCIATED WITH THIS DEGREE.

DEGREE PLAN

ASSOCIATE OF APPLIED SCIENCE IN CYBERSECURITY

Degree Code: 0151 CIP Code: 11.1003

The program is designed for those students seeking career-oriented skills who can identify, assess, and manage cybersecurity threats. The two-year degree prepares students to defend computer operating systems, networks, and data from cyber-attacks.

Program Learning Outcomes for A.A.S. Cybersecurity Program

The Associate of Applied Science in Cybersecurity prepares graduate for entry-level employment and advancement. Students simulate real-world cybersecurity threat scenarios and create opportunities for ethical hacking, security monitoring, analysis and resolution. Students configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization. The program emphasizes the practical application of the skills needed to maintain and ensure secure operational readiness of systems within an organization.

1. Be employable as an associate security analyst, incident responder, network security analyst, or cybersecurity risk analyst.
2. Implement data confidentiality, integrity, availability and security controls on networks, servers, and applications.
3. Develop security principles and policies that comply with cybersecurity laws.
4. Demonstrate critical thinking, complex problem solving, and collaboration.

Students completing the general education core at ASUMH will have demonstrated proficiency in the following skills:

5. Applications of Math and the Natural Sciences appropriate to degree or field of study.
6. Composition and Oral Communication.
7. Evaluation of diverse perspectives and cultures through Arts, Humanities, and Social Sciences.
8. Utilization of technology appropriate to degree or field of study.

Name: _____ Date: _____

Advisor: _____ Student ID# _____

COURSE CODE		COURSE NAME	CREDIT HOURS	HOURS COMPLETED
General Education Requirements (18 credit hours)				
BUSI	21003	Business Communications	3	_____
CPSI	12303	Introduction to Computers	3	_____
ENGL	10103	Composition I (must earn a "C" or better)	3	_____
ENGL	10203	Composition II (must earn a "C" or better)	3	_____
MATH	10133	Applied Math or higher-level mathematics course	3	_____
PLSC	20003	United States Government	3	_____
Business and Computer Core (12 credit hours)				
CPSI	17503	Programming Fundamentals/Logic	3	_____
CPSI	21103	Networking Concepts	3	_____
CPSI	26173	Object-Oriented Programming	3	_____
CPSI	27233	Cybersecurity Essentials	3	_____
Cybersecurity Content (30 credit hours)				
BUSI	23333	Principles of Management **OR**		
BUSI	24443	Project Management	3	_____
CPSI	13374	Ethical Hacking	3	_____
CPSI	21233	Linux	3	_____
CPSI	26533	Computer Forensics	3	_____
CRJU	20243	Cybersecurity Law and Ethics	3	_____
ITEC	11006	CISCO Network Academy I	6	_____
ITEC	12006	CISCO Network Academy II	6	_____
PLSC	23203	Introduction to International Relations	3	_____

Program Total 60 Hours