Information Systems Cybersecurity

Associate of Applied Science
65 credit hours

The Associate of Applied Science in Information Systems (IS) Cybersecurity is designed to introduce students to contemporary information systems security, information assurance and demonstrate how these systems are used throughout global organizations. The focus of this program will be on the key components of information systems assurance and cybersecurity – people, software, hardware, data, security, and communication technologies, and how these components can be integrated and managed to create competitive advantage.

This program is specifically designed to prepare and certify students as Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011and CNSSI No. 4016 Entry Level Risk Analysts or provide current Information Systems professionals with an Information Systems security certification to meet the needs of current and future employer requirements. Upon completion of this program students will receive a university certification of completion, the CompTIA Security+ and EC - Council Certified Ethical Hacker (CEH)™ industry certification in addition to their degree. Key is that the program meets the CAE-2Y curriculum certification by the NSA and complies with the DOD 8570 certification.

The students will participate in the Cybersecurity Challenge Competition with industry partners to demonstrate and apply program knowledge in the capstone class.

Upon program completion students will be able to:

- Apply capable skills to plan, analyze, develop, implement, maintain, and enhance information systems security programs, policies, procedures, and tools to ensure the confidentiality, integrity, and availability of systems, networks, and data.
- Understand and apply knowledge to implement higher-level security requirements; integrate security programs across disciplines; define security plans and policies; assess new system design methodologies to improve software quality; and institute measures to ensure awareness and compliance.
- Knowledge to evaluate and assess new security technologies and/or threats and recommend changes; review and evaluate security incident response policies; and develop long-range plans for IT security systems.
- Understanding and knowledge to resolve integration issues related to the implementation of new systems with the existing infrastructure and why information systems are used today and the technology, people, and organizational components of information systems.
- Understand and analyze various types of information systems provide the information needed to gain business intelligence to support the decision making for the different levels and functions of the organization, the value of information systems investments, how organizations develop and acquire information systems and technologies as well as learn to formulate a business case for a new information system, including estimation of both costs and benefits.
- Understand, apply and evaluate how to secure information systems resources, mitigate risks as well as plan for and recover from disasters, focusing on both human and technological safeguards,

ethical concerns that information systems raise in society, and the impact of information systems on crime, terrorism, and war.

Any student who is ineligible for state, national, or industry licensure is ineligible for entry into this program.

Institutional and Related Course Requirements – 14 hours

UNIV 101 – Freshman Seminar – 3
MATH 104 – Preparatory Algebra – 4
MGT 201 – Principles of Management – 3
STAT 213 – Statistical Methods I – 4

New Mexico General Education Common Core (NMGECC) – 19 hours

I. Communicating Effectively – 9 hours

Required courses:
COMM 101 – Interpersonal Communication – 3
ENG 102 – English Composition – 3
ENG 233 – Writing for Technical Professionals – 3

II. Understanding and Applying Mathematical Principles – 3 hours

Required Course:
MATH 119 – College Algebra – 3

III. Science – 4 hours

Any science with a lab listed in the NMGECC

IV. Social Science – 3 hours

Recommended Courses:
PSCI 102 – American National Government – 3
PSY 101 – Introductory Psychology – 3
SOC 101 – Introductory Sociology – 3
or any Social Science listed in the NMGECC

Technical Requirements – 32 hours

CS 123/L – Programming Fundamentals/Lab – 4
IS 131 – Network Security Fundamentals – 3
IS 136 – Guide to Disaster Recovery – 3
IS 153/L – Introduction of Information Systems – 4
IS 160 – Overview of Operating Systems & Utilities – 3
IS 253 – Firewalls and How They Work – 3
IS 257 – Network Defense and Counter Measures – 3
IS 258 – Cyber Ethics, Professionalism, and Career Development – 3
IS 285 – Ethical Hacking – 3
IS 298 – Programmatic Capstone/Cybersecurity Challenge – 3