Information Systems Cybersecurity
Associate of Applied Science
63-72 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. The National Security Agency and the Department of Homeland Security have designated Eastern New Mexico University-Ruidoso as a National Center of Academic Excellence in Information Assurance/Cybersecurity (CAE-2A). This program is specifically designed to prepare and certify students as Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011 and CNSSI No. 4016 Entry Level Risk Analysts or provide current 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 DOD 8570 certification. 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.
- 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.
- Understand and 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 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.

*Additional hours may be required for program requirements for transfer students who are NMGEC complete.

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

Institutional and Related Requirements – 10 hours

ENGL 1110 – Composition I (3)
FYEX 1110 – First-year Seminar (3)
MATH 1216 – Preparatory Algebra (4)
Note: If institutional/related requirements are waived, additional elective courses will be needed to meet the minimum hours required for the degree.

Program Requirements – 38 – 45 hours

COMM 2120 – Interpersonal Communication (3)*
CS 123/L – Programming Fundamentals/Lab (4)
ENGL 2210 – Professional & Technical Communication (3)
IS 131 – Network Security Fundamentals (3)
IS 136 – Guide to Disaster Recovery (3)
IS 153 – Intro of Information Systems (3)
IS 160 – Overview of Operating Systems & Utilities (3)
IS 253 – Firewalls and How They Work (3)
IS 257 – Ethical Hacking, Computer and Network Defense and Counter Measures (3)
IS 258 – Cyber Ethics, Professionalism, and Career Development (3)
IS 298 – Capstone/Cybersecurity Challenge (3)
MGMT 2110 – Principles of Management (3)
MATH 1220 – College Algebra (4)**
MATH 1350 – Introduction to Statistics (4)

*May be used to satisfy NMGEC Communications requirement.
**May be used to safisfy NMGEC Mathematics requirement.

New Mexico General Education Curriculum (NMGEC)
15-17 hours (as itemized below)

Communicating Effectively – 3 hours
ENGL 1120♦ or 2210♦; COMM 1130♦, 2120, 2140♦

Mathematics – 4 hours
MATH 1130, 1220, 1230, 1350♦, 1510♦

Science – 4 hours
Choose one from* ANTH 1120♦; ASTR 1115/L♦; BIOL1110/L♦, 2110/L♦, 2210/L♦, 2225/L♦, 2310/L♦, 2610/L♦; CHEM 1110C♦, 1215/L♦, 1225/L♦, 121/L♦; GEOL 1110/L♦, 1120/L♦, 123/L 152/L♦; PHYS 113/L♦, 151/L♦, 152/L♦.
*see course description for Math prerequisite

Social and Behavioral Sciences – 3 hours
ANTH 1140♦, 123♦; ECON 1110♦, 2110♦, 2120♦; GEOG 1130♦, 1140♦; POLS 1110♦, 1120♦; PSYC 1110♦; SOCI 1110♦, 2310♦, 215♦.

Flexiable Three – 3 hours
Choose one course from:
Any course from the NMGEC and/or BUSA 1110.

Revised 1.14.20