SUN PATH
New Mexico Skill UP Network
Pathway Acceleration in Technology & Healthcare

NSA/DHS National Centers of Academic Excellence in Cyber Defense
Two-Year Education (CAE-2Y)

Computer and Network Security Certification Program

(*All Courses Online Only)*

Certificate of Completion
18 credit hours

This program meets the CAE2Y knowledge units designation and is specifically designed to prepare students as *Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011 and 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 be receive a university certification of completion and the Industry Certification - CompTIA Security+. Note, the labs use the NDG Netlab virtual labs for hands-on training and the National Cyber League (NCL) Competitions.

IS 153 INTRODUCTION (Foundations) OF INFORMATION SYSTEMS (3) Credits
IS 131 COMPUTER AND SECURITY FUNDAMENTALS. (3) Credits
IS 136 GUIDE TO BUSINESS CONTINUITY AND DISASTER RECOVERY (3) Credits
IS 253 FIREWALLS AND HOW THEY WORK (3) Credits
IS 257 ETHICAL HACKING, COMPUTER AND NETWORK DEFENSE AND COUNTER MEASURES (3) Credits
IS 258 CYBER ETHICS, PROFESSIONALISM, AND CAREER DEVELOPMENT (3) Credits
The objectives of the program include:

- Students are capable of plan, analyze, develop, implement, maintain, and enhancing information systems security programs, policies, procedures, and tools to ensure the confidentiality, integrity, and availability of systems, networks, and data.
- Students will have the 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.
- Students will have the knowledge to 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.
- Students will have understanding and knowledge to resolve integration issues related to the implementation of new systems with the existing infrastructure.

Course Descriptions

Title: IS 131 COMPUTER AND SECURITY FUNDAMENTALS. (3) Credits
Core Course
Catalog description
A comprehensive overview of network security concepts that include: remote access, e-mail, the Web, directory and file transfer, wireless data, common network attacks, cryptography, operational/organizational security, disaster recovery, business continuity, and Cyber Ethics. Students are prepared and take the CompTIA Security + Exam

Title: IS 136 GUIDE TO BUSINESS CONTINUITY AND DISASTER RECOVERY (3) Credits
Core Course
Catalog description
Presents methods to identify vulnerabilities and take appropriate countermeasures to prevent and mitigate failure risks for an organization. It will take an enterprise-wide approach to developing a disaster recovery plan.

Title: IS 153 Introductions (Foundations) of Information Systems (3) Credits
Core Course
Catalog description
Information systems are an integral part of all business activities and careers. This course is designed to introduce students to contemporary information systems and demonstrate how these systems are used throughout global organizations. The focus of this course will be on the key components of information systems - people, software, hardware, data, and communication technologies, and how these components can be integrated and managed to create competitive advantage. Through the knowledge of how IS provides a competitive advantage students will gain an understanding of how information is used in organizations and how IT enables improvement in quality, speed, and agility. This course also provides an introduction to systems and development concepts, technology acquisition, and various types of application software that have become prevalent or are emerging in modern organizations and society. The course introduces Information Assurance and INFOSEC processes. Includes participating in the National Cyber League Competition.

Title: IS 253 FIREWALLS AND HOW THEY WORK (3) Credits
Core Course
Catalog description
This course introduces students to the design and implementation of firewalls. The course covers such topics as firewalls using CISCO Routers, Microsoft server platform and UNIX platform. Focuses on how firewalls function in these environments and the basic steps to plan and implement firewalls. PREREQUISITE: IS 131 or Instructor's permission.

Title: IS 257 ETHICAL HACKING, COMPUTER AND NETWORK DEFENSE AND COUNTER MEASURES (3) Credits
Core Course
Catalog description
This course examines the tools, techniques and technologies used in the technical securing of information assets. Students will receive in-depth information about the software and hardware components of Information Security and Assurance. The students will experience an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus

Creation. When a student leaves this class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council ANSI accredited Certified Ethical Hacker exam 312-50 PREREQUISITE: IS 131

Title: IS 258 CYBER ETHICS, PROFESSIONALISM, AND CAREER DEVELOPMENT (3) Credits
Core Course
Catalog description
This course exposes the student to the topic of Cyber Ethics, Professionalism, and Career Development. The course provides students seeking a career in Cyber Security insight on professional behavior required in a security job and how to develop a professional career in Cyber Security.