COCONINO COMMUNITY COLLEGE
COURSE OUTLINE

Revised by: Sarah Rencher January 12, 2018
Status: Permanent
Effective Term: Fall 2018

A. Identification:
   1. Subject Area: Computer Information Systems (CIS)
   2. Course Number: 237
   3. Course Title: Introduction to Computer Security
   4. Credit Hours: 4
   5. Course Description: Concepts and principles of computer system and data security. Risk mitigation and vulnerabilities, policy formation, control and protection methods, encryption, authentication technologies, host-based and network-based security issues, personnel and physical security issues, issues of law, policy and regulations. Discussions include design, architecture, and implementation, technologies and tools, and techniques for responding to security breaches. The topics covered in this course align with the CompTIA Security+ (SY0-501) certification exam. Prerequisites: CIS 228 or Consent of Instructor. Four Lecture.

B. Course Goals: This course provides the student with a background, foundation, and insights into an overview dimension of the subject of Computer and Information Security. This knowledge will serve as a foundation for future study in selected aspects of this important field or as an important dimension to their effectiveness as an IT security professional.

C. Course Outcomes:
   Upon successful completion of this course, students will be able to:
   1. identify threats, attacks, and vulnerabilities in systems, networks, and information;
   2. install, configure, and troubleshoot technologies and tools to support organizational security;
   3. understand secure network architecture and systems design;
   4. utilize identity and access management concepts;
   5. explain risk management processes and concepts;
   6. explain cryptography algorithms and their basic characteristics.

D. Assessment of Course Outcomes will include:
   1. hands-on lab assessments throughout the semester;
   2. comprehensive final exam.

E. Course Content will include:
   1. threats, attacks and vulnerabilities;
   2. technologies and tools;
   3. architecture and design;
   4. identity and access management;
   5. risk management;
   6. cryptography and PKI.