COCONINO COMMUNITY COLLEGE
COURSE OUTLINE

Prepared by: Ronald D. McFarland Date: September 11, 2012
Status: Experimental Expiration Date: Fall 2014

A. Identification:

1. Subject Area: Computer Information Systems (CIS)

2. Course Number: CIS 137
3. Course Title: Introduction to Computer Security
4. Credit Hrs: 4

Catalog Description: Concepts and principles of computer system and data security. Risks and vulnerabilities, policy formation, controls and protection methods, database security, encryption, authentication technologies, host-based and network-based security issues, personnel and physical security issues, issues of law and privacy. Discussions include firewall design and implementation, secure internet and intranet protocols, and techniques for responding to security breaches. Prerequisites CIS120 and/or CIS130 or Consent of Instructor.

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 in the broader computer information systems and network engineering field. The primary goals of the course are to:

- Understanding of Information Security (InfoSec) principles and approaches
- Understanding of the basic components of InfoSec
- Understanding of basic InfoSec applications
- Ability to remain current with InfoSec literature
- Ability to progress to independent work in the field
- Critically analyze situations of computer use, identifying the issues, consequences and viewpoints.
- Communicate (written and verbally) about a complex, technical topic simply and coherently.

- Work and interact collaboratively in groups to examine, understand and explain key aspects of information security.

C. Course Outcomes:

This course provides the student with a background, foundation, and insights into the full 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 in the broader computer science field.
Students will:

- Understanding of Information Security (InfoSec) principles and approaches
- Understanding of the basic components of InfoSec
- Understanding of basic InfoSec applications
- Ability to remain current with InfoSec literature
- Ability to progress to independent work in the field
- Critically analyze situations of computer use, identifying the issues, consequences and viewpoints.
- Communicate (written and verbally) about a complex, technical topic simply and coherently.
- Work and interact collaboratively in groups to examine, understand and explain key aspects of information security.

D. Assessment of Course Outcomes

Assessment will include:

1. Final Exam covering the Information Security (InfoSec) topics.
2. Final team or individual project of an InfoSec aspect that is comprehensive.

E. Course Content:

Will include:

1. Introduction to Computer Security
2. Cryptographic Tools
3. User Authentication and Access Control
4. Access Control and Database Security
5. Malicious Software and DOS Attacks
6. Intrusion Detection, Prevention Systems and Firewalls
7. Software Security, Buffer Overflow and Programming Security
8. Operating System Security

9. Trusted Computing and Multilevel Security
10. IT Security Management and Risk Assessment
11. IT Security Controls, Plans, and Procedures
12. Physical and Infrastructure Security and Human Resources Security
13. Security Auditing and Legal/Ethical Aspects