COCONINO COMMUNITY COLLEGE
COURSE OUTLINE

Prepared by: Dr. Gonzalo Perez July 18, 2017
Status: Special Topics
Effective: Fall 2017

A. Identification:
   1. Subject Area: Computer Information System (CIS)
   2. Course Number: 298
   3. Course Title: Special Topics: Cybersecurity Fundamentals
   4. Credit Hours: 3
   5. Course Description: This course provides students a comprehensive framework of practices for assuring information security. Students will learn how functions within cybersecurity help support and secure an organization. Content is interwoven with case studies of organizations experiencing the pitfalls of cybersecurity. The course is derived from the Department of Homeland Security's Essential Body of Knowledge (EBK) for IT security, which helps students better understand the structure, roles and competencies in information security.

B. Course Goals: Students will learn how the various roles and functions within cybersecurity practice can be combined and leveraged to produce a secure organization. Concepts will not be presented as stagnant theory; instead, they are interwoven in a real world "adventure" story that runs throughout. This approach grabs students' attention and assists them in visualizing the application of the content to real-world issues that they will face in their professional life. Contemporary cybersecurity breaches will also be examined, and students will work on collaborative projects to better understand new and emerging threats to organizations.

C. Course Outcomes: This course provides the student with a background, foundation, and insights into the full dimension of the subject of cybersecurity. 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.

   Upon successful completion of this course, students will be able to:
   1. describe the core principles and approaches of Cybersecurity;
   2. explain the comprehensive set of practices that are designed to ensure security in cyberspace;
   3. apply the policies of the Security Essential Body of Knowledge (EBK) which is a product of the Department of Homeland Security's National Cybersecurity Division (DHS/NCSD);
   4. demonstrate the ability to remain current with Cybersecurity breaches throughout various organizations;
   5. progress to independent work in the field;
   6. critically analyze case studies of security breaches, identifying the issues, consequences and viewpoints;
   7. communicate (written and verbally) about a complex, technical topic simply and coherently;
   8. work and interact collaboratively in groups to examine, understand and explain key aspects of cybersecurity.

D. Course Outcomes Assessment will include:
   1. grades determined by the instructor as outlined in the class syllabus;
   2. lectures;
   3. discussion;
   4. three examinations;
   5. a group project;
   6. and a number of biometric exercises.

E. Course Content will include:
   1. Information Security
   2. A Global Roadmap for Security
   3. Adapting Best Practice: Tailoring a Solution That Fits
   4. Defining the Company's Executive Roles
   5. Defining the Company's Functional Security Roles
   6. Defining the Corollary Roles for Security
   7. The Data Security Competency
   8. The Digital Forensics Competency
   9. The Enterprise Continuity Competency
   10. The Incident Management Competency
   11. IT Security Training and Awareness
   12. Securing the IT Systems Operations and Maintenance Function
   13. Network and Telecommunications Security
   14. Personnel Security
   15. Physical Security