Computer Science CSC 275
Security, Privacy and Ethics

Credits and Contact Hours: 3 Credits, Contact Hours: 42 (1 contact hour = 50 minutes)

Instructor: Professor Kenneth Atchinson

Textbook:

Course description:

a. Catalog description: This course explores the social issues, including historical and social context, professional responsibilities, risks and liabilities, and intellectual property of an information system organization. Topics include security policy development lifecycle, policy development and implementation process, network security, privacy laws, authentication, and access and information flow controls.
b. Prerequisites: CSC-160
c. Required/Elective:
   a. Computer Information Systems Analyst - Elective
   b. Computer Science – Elective
   c. Network and Computer Systems Analyst – Required
   d. Software Engineering – Required

Specific Goals of Course:

a. Specific outcomes of instruction

   After completion of the course, students will be able to
   i. Know the history of information and information assurance
   ii. Recognize network attacks, threats and vulnerabilities
   iii. Know how malicious code works
   iv. Know how to recognize and apply access controls on data
   v. Know the steps in security auditing, testing and monitoring
   vi. Know how to perform risk assessment, response and recovery
   vii. Know the importance of and how to apply cryptography
   viii. Know current information security standards
b. CAC Criterion 3 outcomes addressed by the course:
   e. An understanding of professional, ethical, legal, security, and social issues and responsibilities.
   g. An ability to analyze the local and global impact of computing on individuals, organizations, and society.

c. EAC Criterion 3 outcomes addressed by the course:
   f. Introduce an understanding of professional and ethical responsibility
   h. Introduce the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
   j. Introduce a knowledge of contemporary issues

Brief list of topics to be covered

a. Introduction to Information Systems Security
b. Current trends in Information Assurance
c. Malicious Attacks, Threats, and Vulnerabilities
d. Access Controls
e. Auditing, Testing, and Monitoring
f. Risk, Response, and Recovery
g. Cryptography
h. Malicious Code and Activity
i. Information Security Standards
j. Information Security Education and Training