Syllabus

CSC 270 Principles of Information Security

General Information

Date

July 31st, 2018

Author

Sandra Brown

Department

Computing Sciences

Course Prefix

CSC

Course Number

270

Course Title

Principles of Information Security

Course Information

Credit Hours

3

Lecture Contact Hours

3

Lab Contact Hours

0

Other Contact Hours

0

Catalog Description

This course is an introduction to the various technical and administrative aspects of Information Security and Assurance. This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. Students will be exposed to the spectrum of Security activities, methods, methodologies, and procedures, technical and managerial responses and an overview of the information security planning and staffing functions.

Key Assessment

This course does not contain a Key Assessment for any programs

Prerequisites

None

Co-requisites

None

Grading Scheme

Letter

First Year Experience/Capstone Designation

This course DOES NOT satisfy the outcomes applicable for status as a FYE or Capstone.

SUNY General Education

This course is designated as satisfying a requirement in the following SUNY Gen Ed category

None

FLCC Values

Institutional Learning Outcomes Addressed by the Course

Vitality
Inquiry
Interconnectedness

Course Learning Outcomes

Course Learning Outcomes

1. Describe the legal, ethical, and professional issues in information security

2. Demonstrate knowledge of security protocols

3. Differentiate between different security devices and practices

Outline of Topics Covered

1. Introduction to Information Security

2. Security Investigation Phase
    a. The need for security
    b. Threats

c. Attacks

3. Legal, Ethical and professional issues in Info Security

   a. Relevant US Laws

   b. International Laws and legal bodies

   c. Policy vs. law

   d. Standards and practices

   e. Info Security blueprints

   f. Security architecture

4. Planning for continuity

   a. Business impact analysis

   b. Incident response planning

   c. Incident reaction

   d. Incident recovery

   e. Disaster recovery planning

   f. Law enforcement involvement

5. Physical Design

   a. Firewalls

   b. IDS

   c. Filters

   d. Cryptography and encryption –based solutions

   e. Access control devices