IT 0120 - INTRODUCTION TO INFORMATION SYSTEMS SECURITY

Catalog Description

Formerly known as CIS 147
Prerequisite: Completion of IT 105 with grade of "C" or better
Advisory: Completion of IT 115 with grade of "C" or better
Hours: 72 (54 lecture, 18 laboratory)
Description: Introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. Addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Preparation for the CompTIA Security+ certification exams. (C-ID ITIS 160) (CSU)

Course Student Learning Outcomes

- CSLO #1: Research, analyze and evaluate information to solve business problems using appropriate network security technology.
- CSLO #2: Design and produce data and computer network security incorporating current trends, security, and best practices.
- CSLO #3: Employ network security concepts and terminology in professional communication.
- CSLO #4: Demonstrate marketable network security career skills.

Effective Term

Fall 2023

Course Type

Credit - Degree-applicable

Contact Hours

72

Outside of Class Hours

90

Total Student Learning Hours

162

Course Objectives

Lecture:
1. Describe the fundamental principles of information systems security.
2. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
3. Evaluate the need for the careful design of a secure organizational information infrastructure.
4. Determine both technical and administrative mitigation approaches.
5. Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).
6. Define basic cryptography, its implementation considerations, and key management.
7. Design and guide the development of an organization's security policy.

Laboratory:
1. Perform risk analysis and risk management.
2. Create and maintain a comprehensive security model.
3. Apply security technologies.
4. Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
5. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

General Education Information

- Approved College Associate Degree GE Applicability
- CSU GE Applicability (Recommended-requires CSU approval)
- Cal-GETC Applicability (Recommended - Requires External Approval)
- IGETC Applicability (Recommended-requires CSU/UC approval)

Articulation Information

- CSU Transferable

Methods of Evaluation

- Objective Examinations
  - Example: Based upon course readings and class discussions relating to encryption, students would be required to take a quiz relating to chapter content, and to explain different encryption methodologies and their resistance to hacking. Example: In your own words (no copy/paste allowed) identify the difference between asymmetric encryption and symmetric encryption using the same key length, highlighting information about strength and performance related to each. Instructor will grade based on level of understanding shown in the response.
- Problem Solving Examinations
  - Example: Students will be provided with a written scenario, outlining a company's current password policy and asked to critique, in writing, the policy, identifying key point in the policy that are acceptable or need to be modified. Key points in terms of evaluation include providing through research information that justifies their analysis of the password policy and includes alternatives relative to what should or should not be implemented. A grading rubric will be provided.
- Projects
  - Example: Given a specific scenario, students would be required to prepare an "incident response plan (IRP)." Student performance would be based upon a rubric designed to incorporate both the requirements of an IRP, as identified course readings, and the clearness of plan response instructions.
- Skill Demonstrations
  - Example: Students will be provided lab assignments based on the weekly topic and required to complete the tasks outlined. See the lab example in 14b for sample. Example: The PGP software will be installed in a lab exercise and students would encrypt and decript messages showing how the software is utilized to convert plain text into cybertext and how to reverse the process (decrypt). Students will capture images to show the process and submit for grading. Grading will be based on a complete set of images with proper notations as described in the instructions. Pass/Fail Grading.

Repeatable

No

Methods of Instruction

- Laboratory
- Lecture/Discussion
- Distance Learning

Lab:

1. Instructor will guide students through hands-on lab exercises to implement the concepts relating to encryption and the utilization of encryption software. The software would be installed in a lab exercise and students would encrypt and decrypt messages showing how the software is utilized to convert plain text into cyphertext and how to reverse the process (decrypt). (Laboratory Objective 3)

Lecture:

1. After students complete weekly reading assignments relating to encryption, the instructor will lead a review discussion on the topics covered. As an example, the instructor will lead a discussion of Pretty Good Privacy (PGP) software. (Lecture Objective 6)

Distance Learning

1. Following an online lecture on passwords, students will be provided with a written scenario, outlining a company's current password policy and asked to critic, in writing, the policy, identifying key point in the policy that are acceptable or need to be modified based upon issues that relate to concerns about privacy, confidentiality, accountability, termination, and other typical business concerns relating to information assurance and cyber defense. (Lecture Objective 7)

Typical Out of Class Assignments

Reading Assignments

1. Students read from the course text. For example students read the textbook chapter on encryption and answer end of chapter questions.
2. Students perform web based research on software and hardware security concepts from sites such as www.cert.org and report back on their findings.

Writing, Problem Solving or Performance

Example 1: After listening to the podcast (or reading the transcript) of a discussion titled "Train for the Unexpected," available at the CERT website (http://www.cert.org/podcast/show/20100330meyer.html), submit a one page response, identifying key information that will help you in your efforts to develop an incident response plan. Example 2: Detail the specific differences between symmetric cryptographic algorithms and asymmetric cryptography algorithms and explain where each algorithm would be utilized.

Other (Term projects, research papers, portfolios, etc.)

Required Materials

- The Official CompTIA Security+ Student Guide (Exam SY0-601)
  - Author: CompTIA
  - Publisher: CompTIA
  - Publication Date: 2020
  - Text Edition:
  - Classic Textbook?: No
  - OER Link:
  - OER:
- CompTIA Security+ Study Guide: Exam SY0-601
  - Author: Mark Chapple
  - Publisher: Sybex
  - Publication Date: 2021
  - Text Edition: 8th
  - Classic Textbook?: No
  - OER Link:
  - OER:

Other materials and-or supplies required of students that contribute to the cost of the course.