**Course Name:** Introduction to Computer Security

**Course Number:** CST* E269

**Credits:** 3

**Catalog description:** A study of the fundamental elements of computer security. The course teaches students how to identify security vulnerabilities in computer systems and how to address these vulnerabilities using industry standard methodologies for securing computer hardware, networks, applications, data, and communications. Course content is continually updated to reflect the current state of the art in computer security.

*The course requires substantial hands-on computer work in a computerized classroom environment.*

**Prerequisite:** The ability to perform basic file management and word processing tasks on a personal computer

**Corequisite or Parallel:**

# General Education Competencies Satisfied:

**HCC General Education Requirement Designated Competency Attribute Code(s):**

**None**

**Additional CSCU General Education Requirements for CSCU Transfer Degree Programs:**

**None**

**Embedded Competency(ies):**

**None**

**Discipline-Specific Attribute Code(s):**

☒ **COMP** **Computer Science Elective**

## Course objectives:

**General Education Goals and Outcomes:**

**None**

**Course Specific Objectives:**

1. Develop a proficiency in interfacing with routers, switches and firewalls.
2. Develop hardware access security – physical / location security.
3. Understand compliance issue that may be imposed by outside sources.
4. Demonstrate how applications, data and host access can be managed through hardware/ software functionality.
5. Demonstrate an understanding of how numerous encryption schemes are implemented in a production environment.
6. Use various vendor monitor tools to understand the health of the hardware / software environment.
7. Develop the ability to recognize specific software / subsystems to support user business requirements.

**Course Content:**

- Practice setting up routers, switches and firewalls for controlling access to secured resources.
- Develop hardware access control for a proposed network control center.
- Investigate threats that can be used against the classroom configuration.
- Build application security through software / hardware controls.
- Secure all data resources, allowing only authorized access via control lists.
- Develop host access security via software controls.
- Use **S**ecured **SH**ell for secure remote login and file transfer
- Transfer files with sFTP.
- Implement advanced security through **A**ccess **C**ontrol **L**ists.
- Design encryption scenarios as a means of protecting transmitted data.
- Set up management reports to show daily system security health.

Date Course Created: Spring 2015

Date of Last Revision: 04/03/2017