The Peninsula's Community College

**Course Content Summary**
**ITN 267 – Legal Topics in Network Security (3 Credits)**

TNCC Cybersecurity Program web page: http://tncc.edu/programs/cyber-security

**Course Description:**

Conveys an in-depth exploration of the civil and common law issues that apply to network security. Explores statutes, jurisdictional, and constitutional issues related to computer crimes and privacy. Includes rules of evidence, seizure and evidence handling, court presentation and computer privacy in the digital age. Lecture 3 hours per week.

**Statement of Purpose:**

This course is designed to train the student on legal, regulatory, and policy standards that impact his or her role as a network administrator or security professional. The course emphasizes common concepts in information security, privacy, the law, and how these concepts affect government and private organizational thinking about information security. The course also provides insight into the creation of an information security program that complies with the laws pertaining to information security. This course also includes content, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria.

**Course Prerequisites / Corequisites:**

ITN 260.

**Required Text:**

Legal Issues in Information Security, latest edition.
Author: Grama, J. L.
Publisher: Jones & Bartlett Learning.

# COURSE OBJECTIVES

Upon completion of this course, the student will have a working knowledge of:

**A.** The fundamental concepts of information security, privacy, and the American legal system
**B.** The security and privacy of government, corporate, and individual information
**C.** Contracts, intellectual property law, and criminal and tort law
**D.** Information security governance, risk analysis, incident response, and contingency planning
**E.** Computer forensics and investigations

# STUDENT LEARNING OUTCOMES

### 1.0 Information Security Overview

1.1 Describe the key concepts associated with information security.
1.2 Describe information security goals and provide examples.
1.3 Describe common information security concerns.
1.4 Describe mechanisms used to protect information security.

### 2.0 Privacy Overview

2.1 Describe basic privacy principles.
2.2 Explain the difference between information security and privacy.
2.3 Describe threats to privacy.
2.4 Explain the important issues regarding workplace privacy.
2.5 Describe the general principles for privacy protection in information systems.

### 3.0 The American Legal System

3.1 Describe the American legal system. **(PL7)**
3.2 Explain sources of law. **(PL8)**
3.3 Distinguish between different types of law.
3.4 Explain the role of precedent.
3.5 Describe the role of regulatory authorities. **(PL8)**
3.6 Explain the difference between compliance and audit.
3.7 Describe how security, privacy, and compliance fit together.

**4.0 Security and Privacy of Consumer Financial Information**

4.1 Describe the business challenges facing financial institutions.
4.2 Define a financial institution and consumer financial information.
4.3 Explain the main parts of the Gramm-Leach-Bliley Act. **(PL4)**
4.4 Explain the role of the Federal Financial Institutions Examination Council.
4.5 Describe the Federal Trade Commission Red Flags Rule. **(PL8)**
4.6 Describe the Payment Card Industry Standards. **(PL6) (PL8)**

**5.0 Security and Privacy of Information Belonging to Children and in Educational Records**

5.1 List some of the challenges with protecting children on the internet.
5.2 Identify the purpose and scope of COPPA, and describe its main requirements and oversight responsibilities. **(PL5) (PL8)**
5.3 Identify the purpose and scope of CIPA, and describe its main requirements and oversight responsibilities. **(PL8)**
5.4 Identify the purpose and scope of FERPA, and describe its main requirements and oversight responsibilities. **(PL1) (PL8)**

**6.0 Security and Privacy of Health Information**

6.1 Describe the business challenges facing the health care industry.
6.2 Explain why health care information is sensitive.
6.3 Explain the main parts of the Health Insurance Portability and Accountability Act. **(PL1)**
6.4 Describe the role of state law in protecting the confidentiality of medical records. **(PL8)**

**7.0 Corporate information Security and Privacy Regulation**

7.1 Describe the difference between public and private companies.
7.2 Explain the history behind the Sarbanes-Oxley Act. **(PL3)**
7.3 Discuss the main requirements of the Sarbanes-Oxley Act. **(PL3)**
7.4 Explain the role of the Public Company Accounting Oversight Board.
7.5 Describe how Section 404 internal control requirements impact information security.
7.6 Discuss frameworks used to guide Sarbanes-Oxley internal control requirements. **(PL3)**

**8.0 Federal Government information Security and Privacy Regulations**

8.1 Describe the federal government's information security challenges. **(PL2)**
8.2 Explain the main requirements of FISMA. **(PL8)**
8.3 Describe the role of the National Institute of Standards and Technology in creating information security standards.
8.4 Describe how the U.S. federal government protects privacy in information systems. **(PL7)**
8.5 Describe how the U.S. Patriot Act impacts privacy in information systems. **(PL9)**
8.6 Explain import and export control laws. **(PL7)**
8.7 Describe how the Americans with Disabilities Act section 508, impacts the federal government information security and privacy challenges. **(PL11)**

## 9.0 State Laws Protecting Citizen Information and Breach Notification Laws

9.1 Describe state approaches to protecting the security of personal information. **(PL7)**
9.2 Describe laws that protect certain types of data. **(PL8)**
9.3 Describe state breach notification laws. **(PL7)**
9.4 Describe the differences between state breach notification laws. **(PL7)**

## 10.0 Intellectual Property Law

10.1 Describe the importance of intellectual property law.
10.2 Explain the basic concept of legal ownership.
10.3 Explain how patents are used and what they protect.
10.4 Explain how trademarks are used and what they protect.
10.5 Explain how copyrights are used and what they protect.
10.6 Describe intellectual property concerns with respect to internet use.
10.7 Describe the Digital Millennium Copyright Act and what it protects.

## 11.0 The Role of Contracts

11.1 Describe traditional contract law principles.
11.2 Describe the main differences between contracting on paper and contracting online.
11.3 Describe shrinkwrap, clickwrap, and browserwrap agreements.
11.4 Describe end-user license agreements.
11.5 Discuss why it's important to include information security provisions in contracts.

## 12.0 Criminal Law and Tort Law Issues in Cyberspace

12.1 Discuss common criminal law concepts.
12.2 Describe the common criminal laws used to prosecute cybercrimes.
12.3 Discuss common tort law concepts.
12.4 Describe common tort principles used in cyberspace.
12.5 Explain the difference between criminal and tort law. **(PL8)**

## 13.0 Information Security Governance

13.1 Describe the key concepts and terms associated with information security governance.
13.2 Describe the goals of different information security governance documents.
13.3 Describe the different types of policies that can be used to govern information security.

## 14.0 Risk Analysis, Incident Response, and Contingency Planning

14.1 Describe the risk assessment process.
14.2 Describe how to create an incident response plan.
14.3 Describe the business continuity planning process.
14.4 Describe how to create a disaster recovery plan.
14.5 Explain the differences between risk assessment, incident response, business continuity planning, and disaster recovery.

## 15.0 Computer Forensics and Investigations

15.1 Define computer forensics.
15.2 Explain the role of a computer forensics examiner.
15.3 Explain why digital evidence must be carefully handled.
15.4 Describe why chain of custody is important.
15.5 Explain the laws that affect the collection of digital evidence.
15.6 Describe concerns regarding the admissibility of digital evidence.

**CAE2Y Knowledge Unit Domain Index**

| Course Content KU Indicator | CAE2Y KU Full Domain Name |
|---|---|
| BD | **Basic Data Analysis** |
| BS | **Basic Scripting** |
| CD | **Cyber Defense** |
| CT | **Cyber Threats** |
| FS | **Fundamental Security Design Principles** |
| IA | **Information Assurance Fundamentals** |
| IC | **Introduction to Cryptography** |
| IT | **Information Technology System Components** |
| NC | **Networking Concepts** |
| PL | **Policy legal Ethics and Compliance** |
| SA | **Systems Administration** |

**NOTE:** the number following the KU Indicator represents the KU Domain topic as shown in the KU mapping matrix (Excel file).