# CSCI 3500 Essentials of Information Security
# 3 Credit Hours CRN: 83446/83447
# Fall 2026

*Dr. Michael Lehrfeld Lehrfeld@etsu.edu*
*2:55-4:50 / 5-6:50 M/W – Brinkley Center 215/230*
*Office Hours: Brinkley Center 151*
*M/W 12:55-2:55*
*T 10:30-12:30*

## Course Overview

This course presents critical concepts and skills that relate to protecting information assets from harm. Topics include the history of information security; basic security-related terminology and concepts; major classes of threats to information security; model strategies for understanding and protecting against those threats; and best practices in information security.

## Course Purpose:

The course seeks to introduce students to the fundamental theory and practice of information security, to raise awareness of information security education among general users.

## Course Goals:

Students completing this course are expected to be able to successfully demonstrate familiarity with the following components:

- Fundamental concepts and terminologies of information security
- Security models and operations
- Security infrastructure
- Ethical and legal issues related to information security

## Prerequisites

C- or better in CSCI 1260 and C- or better in CSCI 2020

## Major Topics

Introduction of history and concepts of information security; security threats, attacks, and hacking; security models; basic concepts of cryptography and public key infrastructure; policies, standards and people; risk management; attacks and malware; e-mail security; intrusion detection and prevention; disaster recovery and organizations policy; ethical issues in information security; computer forensics

## Learning Outcomes

Students completing this course are expected to be able to successfully demonstrate familiarity with the following components:

• Demonstrate an understanding of fundamental concepts and terminologies of information security and privacy.

• Demonstrate an understanding of security access control and data integrity models and identity management.

• Demonstrate an understanding of the critical concerns that need to be addressed by an organization to secure its information assets, including issues related to the facilities and resources that an organization uses.

• Demonstrate an understanding of the fundamentals and basic principles of information security and the impact of physical security on network security.

• Demonstrate an understanding of the role of people and policy in information security.

• Demonstrate an understanding of different kinds of threats to and attacks on information security, including standard forms of malware.

• Demonstrate a basic understanding of intrusion detection systems and security baselines.

• Discuss risk estimation, management, and privacy impact assessment.

• Demonstrate an understanding of the basic concepts of computer forensics.

• Discuss ethical and privacy issues in information security, person identifiable information and anonymity.

## Major Assignments

This class's objectives will be met through the following types of activities:

- assigned readings
- written homework/lab assignments
- quizzes or discussion questions
- exams to assess the students' understanding of the material

**Assignment for Wednesday August 26th start of class**

Please download the VMWare Workstation version of Kali Linux on your laptop (along with VMWare Workstation from here)

Kali → Get Kali | Kali Linux

If you are not using a laptop, please place the unzipped files on an external hard drive. This must be completed prior to class. There will be a quiz grade awarded for completing this by the start of class.

**Graded Assignments (estimated)**

| | | |
|---|---|---|
| Quizzes | 10 | 25% drop lowest grade |
| Exams | 2 | 25% each |
| Labs | 8 | 20% |
| Discussion | 1 | 5% pass/fail |

**Course Topics**

Lecture 1 – Introduction to Security
Lecture 2 – The Need for Security
Lecture 3 – Legal and Ethical Issues
Lecture 4 – Physical Security
Lecture 5 – Risk Management
Lecture 6 – Firewalls
Lecture 7 – Intrusion Detection Systems
Lecture 8 – Cryptography
Lecture 9 – Implementing Security Controls
Lecture 10 – Personnel and Privacy Concerns in Security
Lecture 11 – Planning for a Secure Environment
Lecture 12 – Security Analytics
Lecture 13 – Security Governance
Lecture 14 – Introduction to Forensics

**Lab Write Ups**
The students MUST use the Lab Manual Guide written labs unless noted by the instructor. Failure to do so will result in an automatic zero for the assignment. The guide can be found on D2L.

All Lab write-ups are due by the start of class. No late labs will be accepted.

**Quizzes**
Quizzes will be administered during class. They will consist of questions from the assigned readings, labs, and lectures. Quizzes cannot be made up. Quizzes will be closed notes and book. The lowest quiz grade will be dropped.

**Student Led Class Discussion**
Students will experience researching and sharing security related current information with classmates. Each class period will begin with an assigned team leading a 25-minute discussion about the assigned topic for that class.

The students should provide a short overview of their assigned topic. Then the discussion leaders will embark on a discussion session with the full class participating in analyzing the topic with a focus on current events that directly relate to that topic. Careful consideration should be given to the analysis of the current event and how it relates to the assigned topic. This is not a news report. You should not just re-read the news. Analysis is the key to a successful presentation.

The discussion leaders' grade will be based upon the following rubric:

- Discussion leaders were well prepared.
- Discussion leaders were professional and conducted the overall discussion well.
- Discussion leaders' presented elements were concise, accurate, and interesting.
- Discussion leaders managed class discussion well and achieved good input from the class.
- Discussion leaders motivated everyone to participate in the discussion and created a forum where the entire class (not just a select few) participated.
- Discussion leaders interjected relevant material, where appropriate, from outside the chapter (reference to other class content/articles, current events, personal experience, other research, etc.).
- Discussion leaders managed time effectively.
- *Discussion leaders focused on class-relevant issues and enhanced the class members' knowledge of the material.*
- If you use a video(s) to aid your presentation, total length of all video should not exceed 4 minutes.

**Grading Scale**

| Percentage | Letter |
|---|---|
| 93-100 | A |
| 90-92 | A- |
| 87-89 | B+ |
| 83-86 | B |
| 80-82 | B- |
| 77-79 | C+ |
| 73-76 | C |
| 70-72 | C- |
| 60-69 | D |
| 0-59 | F |

**Attendance Policy**

Each student is expected to attend class. Attendance may be taken each lecture period. After missing your second lecture, each additional absence may result in a one final grade decrement (e.g. A to A-, B+ to B, etc.). You must attend at least two-thirds of a day's scheduled class time to be considered present. Repeated lateness or early departures may be counted as an absence at the discretion of the instructor.

**Academic Integrity Policy**
All activity associated with this course will be in line with the University's applicable policies. Do not confuse the discussion of illegal activities with permission to commit illegal activities. When in doubt, do not do it.

If you are caught plagiarizing, you will be given a zero for the report, your final grade will be reduced by 1 letter grade (B+ to a C+, etc.), and an official report will be entered into your permanent record.

**Recommended Text**
Principles of Information Security, 7th Edition, Michael Whitman and Herbert Mattord; Course Technology; ISBN-13: 978-0-357-50643-1

**Course Topics**

- Introduction to Information Security
- Cryptography and Privacy
- Hash Functions & MAC
- Data Security (at-rest and in-transit)
- Key Distribution, identity verification, and public key infrastructure
- Web & Data Security • Risk management
- Security Models (Bell-La Padula, Biba, etc)
- Access Control and Data Integrity Models and Identity Management
- Firewalls
- Physical Security, Surveillance Laws, Techniques, and Ethics
- Digital Forensics • Intrusion Detection Prevention
- IoT Security
- Privacy Laws, Policies, and Regulations, and legal and ethical matters
- Tracking, Anonymity, and Personally Identifiable Information

**Exams**

Midterm – October 7th
Final – December 7th during class

**Additional Resources**

Students can also find more computer science research materials at Sherrod Library's Research Guide for Computer & Information Sciences (http://sherrod.etsu.edu/tools/rg/computer.html#dblist).

**University Syllabus Attachment**
QR Code PDF Attachment

Link: University Syllabus Attachment Link
URL: https://www.etsu.edu/curriculum-innovation/syllabusattachment.php