CENTRAL TEXAS COLLEGE
SYLLABUS FOR HMSY 1370
INFORMATION TECHNOLOGY SECURITY
FOR HOMELAND SECURITY SPECIALISTS

Semester Hours Credit: 3

INSTRUCTOR: _____
OFFICE HOURS: _____

I. INTRODUCTION

A. Introduction to Information Technology Security for Homeland Security Specialists: is the study of the basics in cyber security with an understanding on how to protect data and infrastructure from the ravages of cyber crimes and electronic terrorism. Topics include desktop computer security, organizational security, communication security, and network security. The course examines applications with proven success and ties them to real-life scenarios.

B. This course is a required course in the Homeland Security and Emergency Management Degree Plan and Certificate of Completion.

C. This course is occupationally related and serves a preparation for careers in Homeland Security.

D. Prerequisite(s): None

II. LEARNING OUTCOMES

Upon successful completion of this course, Information Technology Security, the student will:

1. Describe a comprehensive overview of security challenges.
2. Recognize domestic and international terrorism.
3. Recognize the steps in a comprehensive defense strategy.
4. Explain security issues in verbal and written formats effectively.

III. INSTRUCTIONAL MATERIALS

The instructional materials identified for this course are viewable through www.ctcd.edu/books

IV. COURSE REQUIREMENTS

A. Attend classes.
B. Read all chapters as assigned.
C. Participate in classroom discussions, complete chapter reviews and write short research papers.
D. Be present for all examinations.

V. EXAMINATIONS

A. There will be at least two major examinations.
B. A student should be present for all exams. Students without excused absences will be given a zero for the exam missed.

VI. SEMESTER GRADE COMPUTATION

This is left to instructor choice but might look like:

COURSE REQUIREMENTS	POINTS
Assignments	300
Research Papers	200
Exam 1	200
Exam 2	300
TOTAL	**1000**

POINTS	GRADE	QUALITY POINTS
900-1000	A-Superior	4
800-899	B-Above Average	3
700-799	C-Average	2
600- 699	D- Passing but Unsatisfactory	1
0-599	F-Failure	0

VII. NOTES AND ADDITIONAL INSTRUCTIONS FROM THE INSTRUCTOR

A. Course Withdrawal: It is the student's responsibility to officially withdraw from a course if circumstances prevent attendance. Any student who desires to, or must, officially withdraw from a course after the first scheduled class meeting must file a Central Texas College Application for Withdrawal (CTC Form 59). The student must sign the withdrawal form.

CTC Form 59 will be accepted at any time prior to Friday of the 12th week of classes during the 16-week fall and spring semesters. The deadline for sessions of other lengths is:

10-week session Friday of the 8th week
8-week session Friday of the 6th week
5-week session Friday of the 4th week

The equivalent date (75% of the semester) will be used for sessions of other lengths. The specific last day to withdraw is published each semester in the Schedule Bulletin.

A student who officially withdraws will be awarded the grade of "W" provided the student's attendance and academic performance are satisfactory at the time of official withdrawal. Students must file a withdrawal application with the College before they may be considered for withdrawal.

A student may not withdraw from a class for which the instructor has previously issued the student a grade of "F" or "FN" for nonattendance.

B. Administrative Withdrawal: An administrative withdrawal may be initiated when the student fails to meet College attendance requirements.

C. Incomplete Grade: The College catalog states, "An incomplete grade may be given in those cases where the student has completed the majority of the coursework but, because of personal illness, death in the immediate family, or military orders, the student is unable to complete the requirements for a course . . ." Prior approval from the instructor is required before the grade of "I" (Incomplete) is recorded. A student who merely fails to show for the final examination will receive a zero for the final and an "F" for the course.

D. Cellular Phones and Beepers: Cellular phones and beepers will be turned off while the student is in the classroom or laboratory.

E. American's with Disabilities Act (ADA): Disability Support Services provides services to students who have appropriate documentation of a disability. Students requiring accommodations for class are responsible for contacting the Office of Disability Support Services (DSS) located on the central campus. This service is available to all students, regardless of location. Explore the website at www.ctcd.edu/disability-support for further information. Reasonable accommodations will be given in accordance with the federal and state laws through the DSS office.

F. Instructor Discretion: The instructor reserves the right of final decision in course requirements.

G. Civility: Individuals are expected to be cognizant of what a constructive educational experience is and be respectful of those participating in a learning environment. Failure to do so can result in disciplinary action up to and including expulsion.

H. Absences: Class attendance is mandatory. Absences, for any reason, negatively affect the learning process, the individual student and the class. It is the student's responsibility to keep current with the material being presented in class. Please do not call the Computer Science Department regarding absences from class unless you will miss more than two consecutive days.

I. Degree Progression: Students who receive a grade of "D" are advised not to enroll in the next course for which this course was a prerequisite.

J. Failing Grade: The grade of "F" will be given for academic failure, non-attendance, or scholastic dishonesty.

K. Dishonesty: Plagiarism: Statement and Definition - Though no definition can be wholly inclusive, the following definition sets the boundaries on what is acceptable academic behavior while at CTC: ***Plagiarism is an act in which a student uses someone else's words or ideas without due acknowledgment in order to gain some form of reward.***

Suggested 8-Week Course Schedule

Week	Topics	Chapter Readings	Exams
1	Introduction to Security	Chapter 1	
2	Desktop Security	Chapter 2	
3	Internet Security	Chapter 3	
4	Review Research Paper Due		Mid-term Exam
5	Personal Security	Chapter 4	
6	Wireless Network Security	Chapter 5	
7	Enterprise Security	Chapter 6	
8	Review Research Paper Due		Final Exam

A. Unit One: Chapter 1

1. **Learning Outcomes:** Upon successful completion of this unit, the student will be able to:
a. Describe the challenges of securing information
b. Define information security and explain why it is important
c. Identify the types of attackers that are common today
d. Describe attacks and defenses.

2. **Learning Activities:**
a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. **Lesson Outline:**
a. Unit Outline: Follow the sequence of unit learning outcomes.

B. Unit Two: Chapter 2

1. **Learning Outcomes:** Upon successful completion of this unit, the student will be able to:
a. Define what makes a weak password.
b. Describe the attacks against passwords.
c. Identify the different types of social engineering attacks.
d. Describe identity theft and risks of using social networking.
e. Describe personal security defenses.

2. **Learning Activities:**
a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. **Lesson Outline:**
a. Unit Outline: Follow the sequence of unit learning outcomes.

C. Unit Three: Chapter 3

1. **Learning Outcomes:** Upon successful completion of this chapter, the student will be able to:
a. Define malware.
b. List the different types of malware.
c. Identify payloads of malware.
d. Describe the steps for securing software.
e. Explain how to create data backups.

2. **Learning Activities:**
a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. **Lesson Outline:**
a. Unit Outline: Follow the sequence of unit learning outcomes.

D. Unit Four: Chapter 4

1. **Learning Outcomes:** Upon successful completion of this chapter, the student will be able to:

a. Explain how the Internet and email function.
b. Describe how attackers can use browser vulnerabilities, malvertising, and drive-by downloads to spread malware.
c. List the security risks with using email.
d. Describe how to use web browser settings and browser additions to create stronger security.
e. List several Internet security best practices.

2. **Learning Activities:**

a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. **Lesson Outline:**

a. Unit Outline: Follow the sequence of unit learning outcomes.

E. Unit Five: Chapter 5

1. **Learning Outcomes:** Upon successful completion of this chapter, the student will be able to:

a. Describe attacks through Wi-Fi and Bluetooth networks.
b. Explain the different types of attacks on mobile devices.
c. List the defenses for a home Wi-Fi network.
d. Describe how to use a public wireless network securely.
e. List the types of security for mobile devices.

2. **Learning Activities:**

a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. **Lesson Outline:**

a. Unit Outline: Follow the sequence of unit learning outcomes.

F. Unit Six: Chapter 6

1. **Learning Outcomes:** Upon successful completion of this chapter, the student will be able to:

a. Define privacy and explain the risks associated with unprotected private data.
b. Define cryptography.
c. List the various ways in which cryptography is used.
d. Explain how privacy best practices may be used.
e. Describe the responsibilities of organizations regarding protecting private data.

2. Learning Activities:

a. Classwork/discussion
b. Student homework and study
c. Reading assignments

3. Lesson Outline:

a. Unit Outline: Follow the sequence of unit learning outcomes.