CENTRAL TEXAS COLLEGE
ITSY 1342
INFORMATION TECHNOLOGY SECURITY

Semester Hours Credit: 3

INSTRUCTOR: _____

OFFICE HOURS: _____

I. INTRODUCTION

A. Instruction in security for network hardware, software, and data, including physical security, backup procedures, relevant tools, encryption, and protection from viruses. This course also assists individuals in preparing for the Computing Technology Industry Association (CompTIA) Security+ certification exam and a career as a network professional.

B. This course serves as a required or elective course on various degree plans. Curriculum plans for degrees and certificates are listed in the current Central Texas College catalog.

C. The delivery method of this course may be traditional lecture/lab, blended lecture/lab, or online.

D. Prerequisites: ITNW1358 or ITCC1414 or concurrent enrollment in either.

II. LEARNING OUTCOMES

Upon successful completion, Information Technology Security, the student will be able to:

A. Identify and define National Institute of Standards and Technology (NIST) Guidelines and other best practices (C3, C5, C15, C18)
B. Develop backup/recovery procedures to provide for data security (C1, C3, C5, C6, C8, C11, C13, C17, C18, C20)
C. Use network operating system features to implement network security (C8, C17, C18, C19, F1, F7, F9, F12)
D. Identify computer and network threats and vulnerabilities and methods to prevent their effects (C3, C8, C18, C19, C20, F7, F8, F11)
E. Use tools to enhance network security (C5, C6, C8, C11, C15, C18, C19, F1, F8, F9)
F. Use encryption techniques to protect network data (C5, C6, C8, C11, C15, C18, C19, F1, F8, F9)

III. INSTRUCTIONAL MATERIALS

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

B. **Lecture Classes also require at least one USB storage device. Online students may use cloud based storage.**

IV. COURSE REQUIREMENTS

A. **Attend both lecture and lab or in the case of online delivery, be actively engaged in Blackboard and maintain constant progress.**

B. **Be prepared to participate in discussion, team projects/assignments and take unannounced assessments relating to the lecture materials.**

C. **Complete all exams/assessments.**

D. **Submit all assignments on time.**

V. ASSESSMENTS

A. **Student content mastery will be evaluated in the following areas:**

- **Assessments (midterm exam, quizzes, projects, discussion etc.)**
- **Final Assessment (final exam and/or semester project, participation)**

B. **Scheduled and unscheduled assessments will be given at the discretion of the instructor.**

C. **Exams/assessments may be composed of both subjective and objective questions plus computer output.**

D. **A student must take all exams/assessments. Both online and on campus students who know in advance that they will be absent due to school sponsored trips, military duty or orders, or any other valid reason, must arrange to take an early exam/assessment. Unexpected absences due to illness or other extenuating circumstances will require the student to contact the instructor about make-up work in lieu of the missed exam/assessment.**

E. **Students with unexcused absences will be given a zero for each missed assignment.**

VI. SEMESTER GRADE COMPUTATION

Course Requirements	Points
Assignments	300
Assessments	300
Final Assessment	400
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. Information on the following Academic Policies, as described in the CTC Course Catalog will be followed:

1. **Withdrawals**
2. **Grading**
3. **Class Attendance and Course Progress**
4. **Scholastic Honesty**

B. Cell Phones and Pagers: Students will silence cell phones and mobile devices while in the classroom or lab.

C. Americans with Disabilities Act (ADA): Disability Support Services provide 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. Review 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.

D. Instructor Discretion: The instructor reserves the right of final decision in course requirements and may make changes to the course outline and/or assignments as needed.

E. Civility: Individuals are expected to be aware 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.

VIII. COURSE OUTLINE

A. Lesson One:

1. **Learning Outcomes: Upon successful completion of this lesson 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. **Identify how to defend against attacks**
   e. **Define attacks using malware**
   f. **Define social engineering attacks**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Introduction to Security**
   b. **Malware and Social Engineering Attacks**

B. Lesson Two:

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Define Cryptography**
   b. **Define Cryptography Algorithms**
   c. **Explain Cryptography Attacks**
   d. **Define how to use Cryptography**
   e. **Describe how to implement Cryptography**
   f. **Defining, managing types of Digital Certificates**
   g. **Define Public Key Infrastructure (PKI)**
   h. **Identifying Cryptographic Transport Protocols**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Basic Cryptography**
   b. **Advanced Cryptography and PKI**

C. **Lesson Three**

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Explain Networking-Based Attacks**
   b. **List the different types of Server Attacks**
   c. **List the different types of network security devices and how they can be used**
   d. **Describe Security through Network Architecture**
   e. **Explain how network technologies can enhance security**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Networking and Server Attacks**
   b. **Network Security Devices, Design, and Technology**

D. **Lesson Four:**

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **List and describe the functions of common network protocols**
   b. **Identify placement of security devices and technologies**
   c. **Analyzing and identifying issues in security data**
   d. **Managing and Securing Network Platforms**
   e. **Define the different types of wireless attacks**
   f. **Identify Vulnerabilities of IEEE Wireless Security**
   g. **Explain the different wireless security solutions**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**

c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Administering a Secure Network**
   b. **Wireless Network Security**

E. Lesson Five:

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Explain the different ways to apply client security**
   b. **List the ways to apply physical security**
   c. **Explain the solutions for application security**
   d. **List and compare the different types of mobile devices and deployment**
   e. **Explain the risks associated with mobile devices**
   f. **List ways to secure a mobile device**
   g. **Explain how to secure embedded systems and the internet of things**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Client and Application Security**
   b. **Mobile and Embedded Device Security**

F. Lesson Six:

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Describe the different types of authentication credentials**
   b. **Explain what single sign-on can do**
   c. **Describe how to differentiate common account management practices**
   d. **Define access control and access control models**
   e. **Describe how to manage access through account management**
   f. **Explain the best practices for access control**
   g. **Describe how to implement access controls**
   h. **Identify identity and access services**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Authentication and Account Management**
   b. **Access Management**

G. Lesson Seven:

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Assessing the Security Posture**
   b. **Explain vulnerability scanning**
   c. **Describe penetration testing**
   d. **Explain how to practice data privacy and security**
   e. **Define business continuity**
   f. **Describe fault tolerance through redundancy**
   g. **Explain environmental controls**
   h. **Define forensics, the incident response plan and procedures**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   a. **Vulnerability Assessment and Data Security**
   b. **Business Continuity**

H. Lesson Eight:

1. **Learning Outcomes: Upon successful completion of this lesson the student will be able to:**
   a. **Explain how to manage risk**
   b. **Describe the strategies for reducing risk**
   c. **Define the practices for reducing risk**
   d. **Describe how to troubleshoot common security issues**

2. **Learning Activities:**
   a. **Participate in collaborative discussions based on the assigned reading materials. (C9,C12,C14,F1, F2, F5, F6)**
   b. **Complete assigned PC Labs and Case Studies (C18, C19, C20, F8, F9, F11)**
   c. **Submit assigned papers and/or projects (C5, C6, C8, F1, F2, F7, F9, F11)**

3. **Unit Outline:**
   Risk Mitigation