I. INTRODUCTION

A. This course provides in-depth coverage of incident response and incident handling, including identifying sources of attacks and security breaches; analyzing security logs; recovering the system to normal; performing postmortem analysis; and implementing and modifying security measures.

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: Six (6) semester hours of Information Technology Security (ITSY) coursework.

II. LEARNING OUTCOMES

Upon successful completion of this course, Incident Response & Handling, the student will be able to:

A. Identify sources of attacks (C5, C15, C18, F9)
B. Restore the system to normal operation (C5, C15, C18, F9)
C. Identify and prevent security threats (C5, C15, C18, F9)
D. Perform a postmortem analysis (C5, C15, C18, F9)
E. Identify computer investigation issues (C5, C15, C18, F8)
F. Identify the roles and responsibility of the incident response team (C5, C15, C18, 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. (2-4 GB preferred).

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

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Points</th>
<th>Points</th>
<th>Grade</th>
<th>Quality Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>300</td>
<td>900----</td>
<td>A-Superior</td>
<td>4</td>
</tr>
<tr>
<td>Assessments</td>
<td>300</td>
<td>800----</td>
<td>B-Above Average</td>
<td>3</td>
</tr>
<tr>
<td>Final Assessment</td>
<td>400</td>
<td>700----</td>
<td>C-Average</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>600-699</td>
<td>D-Passing, but unsatisfactory</td>
<td>1</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
<td>0-599</td>
<td>F-Failure</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

For non-GoArmyEd active military students, the effective date of withdrawal is the filing date with the Education Center. For all other students, the effective date of withdrawal is the date that the withdrawal application is received by the Central Texas College representative.

Students who used financial aid, military tuition assistance, VA benefits, or other non-personal funds may be required to repay tuition and fees to the funding agency. For specific repayment requirements, contact the Office of Student Financial Aid or Veterans Services Office before withdrawing. Military tuition assistance students should visit their military Education Center or Navy College Office.

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 a grade of “F,” “FI,” “FN,” “IP,” or “XN.”

B. Instructor Initiated Withdrawals: Faculty are authorized to withdraw students who are not making satisfactory course progress to include failure to meet College attendance requirements as outlined in the section of the Catalog entitled “Satisfactory Progress Standards.” The instructor will assign the appropriate grade on CTC Form 59 for submission to the registrar.

Students enrolled in distance learning courses are expected to maintain constant progress throughout the course. Failure to do so may result in the student being administratively withdrawn by the instructor.

Students who have not attended class by the 12th class day of a 16-week course or the 6th class day of an 8-week term may be administratively withdrawn by the instructor with a grade of "W." Students may also be administratively withdrawn from any class when their absences exceed a total of four class meetings for a 16-week course or three class meetings for less than 16-week courses and; in the opinion of the instructor, the student cannot satisfactorily complete the course. In a distance learning course the last date of attendance is the last activity by the student in the course.

C. Administrative Withdrawal: A student may be administratively withdrawn by a designated member of the administrative staff of the College when the student has been placed on Academic Suspension or Disciplinary Suspension; the student has an outstanding financial obligation owed to the college; or the student registered for a course without the required prerequisite or departmental permission.

The College is under no obligation to refund tuition and fees, or other costs associated with an administrative or instructor initiated withdrawal.

D. 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 “IP” for Incomplete is recorded.

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

F. 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.

G. **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.

H. **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.

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” or “FN” will be given for academic failure, non-attendance or scholastic dishonesty.

K. **Scholastic Honesty**: All students are expected to maintain the highest standards of scholastic honesty in the preparation of all course work and during examinations. The college policy on scholastic honesty, including definitions on plagiarism, collusion, and cheating can be found at the following URL: [http://online.ctcd.edu/plagiarism.cfm](http://online.ctcd.edu/plagiarism.cfm)
VIII. COURSE OUTLINE

A. **Unit One: Forensics**

1. **Learning Outcomes:** After completing this unit, you will be able to understand:
   a. The definition and importance of computer forensics
   b. Different types of digital evidence and how they are used
   c. The skills, training, and education required to become a computer forensics investigator
   d. Job opportunities in the field of computer forensics
   e. The history of computer forensics
   f. Agencies in the U.S. and internationally involved in computer forensics investigations

2. **Learning Activities:**
   a. Read Chapter 1 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities

B. **Unit Two: Computer Hardware and Software**

1. **Learning Outcomes:** Upon completion of this Unit, you will be able to understand:
   a. What an operating system is
   b. What binary, decimal, and hexadecimal are and how to convert from each notation
   c. The physical structure of a hard drive and how files are stored and retrieved
   d. The booting process
   e. The Windows file systems
   f. The different features of each Windows operating system and their implications on investigations
   g. The importance of being able to recognize different types of computer hardware
   h. The various disk drive interfaces that an investigator can encounter
   i. The types of devices used to forensically extract data from different storage devices
   j. The variety of storage media used and how this evidence should be handled and analyzed
   k. The use of storage media in actual investigations

2. **Learning Activities:**
   a. Read Chapter 2 and 3 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities
C. **Unit Three: Evidence**

1. **Learning Outcomes:** At the end of this Unit, students should be able to understand:
   a. What is needed to have a computer forensics laboratory certified
   b. Good practices for managing and processing evidence in a computer forensics laboratory
   c. How a computer forensics laboratory should be structured
   d. Computer forensics laboratory requirements for hardware and software
   e. Proper ways to acquire, handle, and analyze digital evidence
   f. Methods of investigating financial fraud
   g. How to use UNIX commands to scour files for particular information of interest

2. **Learning Activities:**
   a. Read Chapter 4 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities

D. **Unit Four: Investigations**

1. **Learning Outcomes:** At the end of this chapter students should be able to understand:
   a. How to gather personal data about a suspect from a variety of online sources
   b. Databases available to law enforcement to profile a suspect
   c. Different types of online crime and how criminal investigations are conducted online
   d. How to capture Internet communications, video, images, and other content to add to an investigation report
   e. Obtaining evidence from a service provider
   f. Documenting a crime scene
   g. Seizing evidence
   h. Documenting and handling evidence
   i. Forensic tools for documenting an investigation
   j. Report writing
   k. The role of an expert witness
   l. Standard operating procedures

2. **Learning Activities:**
   a. Read Chapter 5 and 6 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities
E. **Unit Five: Digital Evidence**

1. **Learning Outcomes:** At the end of this Unit students should be able to understand:
   a. The structure of the legal system in the United States
   b. The role of constitutional law in computer forensics
   c. Principles of search and seizure of computers and other digital devices
   d. Rules for the admissibility of evidence at trial
   e. Case law concerning the use of digital surveillance devices by law enforcement
   f. Cases of computer forensics gone wrong
   g. Structure of the legal system in the European Union
   h. Data privacy and computer forensics in the European Union

2. **Learning Activities:**
   a. Read Chapter 7 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities

F. **Unit Six: Network/Mobile Forensics**

1. **Learning Outcomes:** At the end of this Unit students should be able to understand:
   a. The importance of network forensics
   b. Hardware devices that contain network logs that are valuable to a forensics examiner
   c. IPv4 and IPv6
   d. The OSI Model
   e. Mistakes made when investigating networks
   f. Advanced persistent threats: perpetrators, vectors of attack, and indicators of compromise
   g. How to investigate a network intrusion
   h. The evolution and importance of cellphone forensics
   i. An overview of cellular networks
   j. The type of evidence available from cellphone carriers
   k. Retrieving evidence from a smartphone
   l. Conducting SIM card forensics
   m. Analyzing cellphone operating systems
   n. Legal considerations associated with cellphone investigations
   o. Tables, GPS, and other mobile device forensics
   p. How to document a cellphone investigation

2. **Learning Activities:**
   a. Read Chapter 8 and 9 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)
3. **Unit Outline:** Follow the learning activities

G. **Unit Seven:** Photographs

1. **Learning Outcomes:** At the end of this Unit students should be able to understand:
   a. The use of photograph images by social media users
   b. The metadata found in photograph images
   c. Different types of digital photograph files
   d. Admissibility of photographs in the courtroom
   e. Case studies involving the use of photographic evidence

2. **Learning Activities:**
   a. Read Chapter 10 (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities

H. **Unit Eight:** Macs and Case Studies

1. **Learning Outcomes:** At the end of this Unit students should be able to understand:
   a. The importance of Mac forensics
   b. History of Apple devices
   c. Apple file systems: HFS and HFS+
   d. Virtual files on a Macintosh computer
   e. Property lists (PLists) and their value to investigators
   f. Applications and their associated files
   g. Hardware and software forensics tools for Macintosh computers and iOS devices
   h. How to examine Apple mobile devices
   i. The importance of computer forensics in proving intent to commit a crime
   j. How computer forensics is used at trial and the types of objections that may arise
   k. The role of computer forensics examiner as an expert witness
   l. How digital forensics can potentially be used in any type of investigation or court proceeding
   m. The problem of cyberbullying and digital evidence used to investigate these types of crimes
   n. Anti-cyberbullying legislation
   o. How the use of digital files was used and challenged in the investigation of steroid use by MLB players

2. **Learning Activities:**
   a. Read Chapter 11 and 12 (C5, C6, C8, C19, F1, F5, F11)
b. Complete the assigned quiz and assignment (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the learning activities