AMBERTON UNIVERSITY

e-COURSE SYLLABUS

MIS4360.E1 Introduction to Cybersecurity
Fall 2026

PROFESSOR INFORMATION:

Professor:	Dr. Felix Hernandez
Amberton Extension:	972-279-6511
Amberton Email:	**FHernandez**@amberton.edu

COURSE INFORMATION:

MIS4360.E1	Introduction to Cybersecurity
Level:	Undergraduate
Beginning Date of Session:	Saturday, September 12, 2026
Ending Date of Session:	Thursday, November 19, 2026

Student access available to the Student Portal: Saturday, September 12, 2026

Students enrolled in distance learning courses are not assessed any additional fees for security or identity verification.

PREREQUISITES:
None

TEXTBOOK(S) AND REQUIRED MATERIALS:

Title:	CompTIA Security+ Guide to Network Security Fundamentals
Author:	Mark Ciampa
Publisher:	Cengage Learning
Year Published:	2025
Edition:	8th Edition
ISBN:	10: 9798214000633 or 13: 9798214406978
Price:	Available at http://amberton.ecampus.com

Students should verify enrollment in course before purchasing textbooks. Textbook information and ordering options are available through the Amberton Virtual Bookstore. Since no books are sold on campus, students should plan accordingly and purchase their books in advance of the first day of class, allowing time for shipping.

APA REQUIREMENT:

APA (American Psychological Association) style is most commonly used to cite sources within the social sciences. This resource, revised according to the 7th edition, offers examples for the general format of APA research papers, in-text citations, endnotes/footnotes, and the reference page. For more information, please consult the Publication Manual of the American Psychological Association, (7th ed.). All coursework at Amberton University will comply with the standards contained in the APA Publication Manual.

COURSE COMPETENCIES:
The following represents the course competencies for this class. Competencies are equivalent for all lectures and distance learning courses. Following each competency is the assignment used to gain mastery of this area of study.

This course provides a comprehensive introduction to cybersecurity principles, technologies, and practices for both managerial-level learners and hands-on practitioners. Students explore foundational concepts such as security governance, policy, risk management, legal/ethical standards, and the growing role of AI/ML in modern cyber defense. The course examines network and cloud security architectures, intrusion detection systems, identity and access management, automation tools, cyber threat intelligence, and the fundamentals of ethical hacking. Learners gain practical exposure to incident response, digital forensics, log analysis, and AI enabled security operations. By the end of the course, students will understand key security concepts, evaluate risks, analyze threats, and apply defensive techniques in realistic cybersecurity scenarios.

UPON COMPLETION OF THE COURSE, THE STUDENT WILL BE COMPETENT IN:
1. Explaining foundational cybersecurity principles, governance frameworks, and legal/ethical considerations.
2. Evaluating organizational risk using standard risk-management methodologies and recommending appropriate mitigation strategies.
3. Analyzing network and cloud security architectures, including firewalls, IDS/IPS, segmentation, and identity/access controls.
4. Applying basic skills in intrusion detection, security monitoring, and automation scripting to support cybersecurity operations.
5. Implementing core identity and access management (IAM) concepts, including authentication, authorization, and privilege management.
6. Assessing cyber threats using threat-intelligence frameworks, adversary tactics, and red/blue team methodologies.
7. Demonstrating introductory ethical hacking techniques within authorized laboratory environments.
8. Performing foundational incident-response tasks, including detection, containment, eradication, and recovery procedures.
9. Conducting basic digital forensics processes such as evidence handling, imaging, preservation, and file-system examinations.
10. Analyzing log data from various sources to identify anomalies, security events, and potential indicators of compromise.
11. Identifying how AI/ML supports modern cybersecurity operations, including automated threat detection, SOAR workflows, and behavioral analytics.
12. Integrating cybersecurity concepts to evaluate realistic scenarios and propose appropriate defensive strategies and solutions.

ACQUIRED SKILLS
1. Understand and apply cybersecurity governance frameworks.
2. Analyze network, cloud, and endpoint defensive architectures.
3. Perform intrusion detection and automation scripting.
4. Examine cyber threats using intelligence and red/blue methodologies.
5. Demonstrate ethical hacking fundamentals.
6. Conduct basic digital forensics investigations.
7. Explain how AI/ML supports SOC operations and automated threat detection.

COURSE POLICIES:

STUDENTS' RESPONSIBILITIES:
This syllabus contains information, policies, and procedures for a specific course. By enrolling, the student agrees to read, understand, and abide by the policies, rules, regulations, and ethical standards of Amberton University as contained in the current university catalog and schedule of classes.

ATTENDANCE POLICY:
Regular and punctual class attendance and engagement is expected at Amberton University. In case of an absence, it is the student's responsibility to contact the professor as soon as possible. If a student intends on Withdrawing from a course, it is the student's responsibility to follow the university's policy on formally withdraw from a course. **Ceasing to attend classes does not constitute an official withdrawal.**

Attendance on a lecture course is defined as punctual arrival to, and engagement in, a full lecture session. A Students in a lecture course miss more than 20% (two class periods for weekday classes or one class period for Saturday classes) of the class meetings may be assigned a grade of an "F" or withdrawn at the discretion of Amberton University.

Attendance on a distance learning course is defined as active participation in the weekly online class sessions. "Active participation" can be defined as: submitting an academic assignment, taking an exam, engaging in an interactive tutorial, participating in an online discussion forum (or chat session), or initiating (or responding to) a communication with a faculty member about an academic assignment or the subject matter of the course. A student not meeting these requirements may be assigned a grade of an "F" or withdrawn at the discretion of Amberton University.

PLAGIARISM POLICY:
Plagiarism is the presentation of someone else's work as though it were your own. If you use another person's words, ideas, or information; or if you use material from an outside source – whether a book, magazine, newspaper, business publication, broadcast, speech, or electronic media – you must acknowledge that source. Plagiarism is a violation of the University's code of student ethical conduct and is one that is taken seriously. Amberton University operates on an honor system; therefore, honesty and integrity are essential characteristics of all who are associated with the institution. All Amberton students are expected to abide by the honor system and maintain academic integrity in all their work. Amberton University and its instructors monitor student work for plagiarism and reserve the right to submit such work to technology-based plagiarism detection services and applications at any time.

Self-plagiarism means reusing work that you have already published or submitted for a class. It can involve:

- Resubmitting an entire paper
- Copying or paraphrasing passages from your previous work

Self-plagiarism misleads your readers by presenting previous work as completely new and original. Students may not submit the same paper in substance in two or more classes without prior written permission of the instructors involved.

Amberton University students who use Artificial Intelligence (AI) generated content must adhere to the following policies:

Originality: Students must avoid presenting AI generated content as their own original work. It is essential to acknowledge the involvement of AI in the content creation process in order to maintain academic and ethical standards.
Paraphrasing: When using AI generated content, students must rephrase and/or modify the generated text. Paraphrased AI generated content should also be properly cited.
Acknowledgement: When using AI generated content in any assignment, proper credit must be given to the AI system that generated the content. https://apastyle.apa.org/blog/how-to-cite-chatgpt

Students agree that by taking this course, all required assignments may be subject to submission for a textual similarity review to Turnitin.com for the detection of plagiarism and self-plagiarism. All submitted papers will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism in future papers. Use of Turnitin.com service is subject to the Usage Policy posted on the Turnitin.com website.

Turnitin is a writing improvement and plagiarism prevention tool which uses special algorithms, to compare text-based student submissions to the Turnitin database and other online sources. Turnitin produces a detailed **similarity report** that can be customized and viewed by instructors and students.

Turnitin "Draft Coach" is a Google based add-on to Turnitin which supports students in developing high-quality academic writing; and serves as an integrity coach. Draft Coach helps address errors and improve the quality of student's writing by highlighting grammar mistakes, identifying incorrectly cited sources, and scanning for similarity across several databases. By providing formative feedback on how to address citation issues, incorrect grammar, and matches with the Turnitin database, Draft Coach provides explanations to help students become more confident writers, capable of producing higher quality work both in academics and in the workplace.

COURSE OUTLINE AND CALENDAR:

Week	Topic	Assignment	Competencies/Outcomes	Due Date
Sep 12-Sep 13	Review the course materials and navigate through the course	Introduction discussion	Foundational cybersecurity awareness; course expectations	Sep 13

Sep 14-Sep 20	Module 1: Introduction to Information Security Module 2: Pervasive Attack Surfaces and Controls	Discussion #1 Quiz #1	Foundational cybersecurity principles; governance frameworks; risk awareness; attack surface analysis	Sep 20
Sep 21-Sep 27	Module 3: Fundamentals of Cryptography Module 4: Advanced Cryptography	Assignment #1 Quiz #2	Cryptographic concepts; data protection; secure communications; applied cryptography	Sep 27
Sep 28-Oct 4	Module 5: Endpoint Vulnerabilities, Attacks, and Defenses Module 6: Mobile and Embedded Device Security	Discussion #2 Quiz #3	Endpoint security; mobile and IoT risks; vulnerability analysis; defensive strategies	Oct 4
Oct 5-Oct 11	Module 7: Identity and Access Management (IAM) Module 8: Infrastructure Threats	Case study #1 Quiz #4	IAM implementation; authentication and authorization; security	Oct 11

	and Security Monitoring		monitoring; intrusion detection	
Oct 12-Oct 18	Review Modules 1– 8	Midterm Examination	Integrated understanding of foundational security, cryptography, IAM, and infrastructure defense	Oct 18
Oct 19-Oct 25	Module 9: Infrastructure Security Module 10: Wireless Network Attacks and Defenses	Discussion #3 Quiz #5	Network security architectures; wireless threats; mitigation strategies; defensive controls	Oct 25
Oct 26-Nov 1	Module 11: Cloud and Virtualization Security Module 12: Vulnerability Management	Assignment #2 Quiz #6	Cloud security models; virtualization risks; vulnerability assessment and remediation	Nov 1
Nov 2-Nov 8	Module 13: Incident Preparation and Investigation Module 14: Oversight and Operations	Case Study #2 Quiz #7	Incident response lifecycle; digital forensics basics; operational security oversight	Nov 8
Nov 9-Nov 15	Module 15: Information Security Management	Discussion (Reflection) Quiz #8	Security governance; risk management; asset management; strategic security leadership	Nov 15
Nov 16- Nov 19	Review Modules 9–15	Final Examination	Comprehensive integration of cybersecurity principles, applied skills, and strategic analysis	Nov 19

GRADING CRITERIA:

Grading Scale:

Discussion (15% of final grade | 5 discussion activities)

- Discussion activities are assigned throughout the course to encourage interaction, collaboration, and engagement among students.
- Assesses participation, critical thinking, clarity of communication, and the ability to apply course concepts in academic and professional discussions.

Quiz (10% of final grade | 8 quizzes)

- Quizzes are administered periodically to reinforce weekly learning objectives and ensure continuous engagement with course content.
- Evaluates understanding of key terminology, foundational concepts, and assigned course materials.

Assignment – Case Study (20% of final grade | 2 case study assignments)

- Case study assignments require students to analyze real-world or hypothetical business situations using course concepts.
- Assesses analytical thinking, application of theoretical frameworks, written communication, and problem-solving skills.

Assignment – Scenario-Based Problem Solving (20% of final grade | 2 scenario-based assignments)

- Scenario-based assignments focus on decision-making in practical, applied, and professional contexts.
- Evaluates the ability to interpret information, apply course concepts, justify decisions, and develop effective solutions.

Midterm Examination (15% of final grade | 1exam)

- An examination covering material from the first half of the course.
- Measures understanding of core concepts, theories, and applied knowledge.

Final Examination (20% of final grade | 1 comprehensive exam)

- A comprehensive exam administered at the end of the course covering all course material.
- Assesses overall knowledge integration, critical thinking, and mastery of course learning outcomes.

Undergraduate
90 – 100 A
80 – 89 B
70 – 79 C
60 – 69 D
Below 60 F

GRADE NOTIFICATION AND INSTRUCTOR FEEDBACK:
Students should review instructor feedback provided through Moodle or Amberton CampusWeb Portal. Final grades are processed approximately one week after the session and may be viewed through the student portal. Grades will not be released by phone or through unsecured channels. University instructors will not leave a message with comments or grades in any type of media that is not secure.

For questions regarding grades after the semester has ended, students should use their university email account and contact the instructor at the faculty email address as provided above in Professor Information area.

INCOMPLETE GRADES:
An "I" (Incomplete) grade is granted only at the professor's discretion for emergencies or illness.

Students have 30 days from the end of the session to complete the course requirements. If the conditions are not met within this 30-day window, the "I" automatically converts to an "F".

HOW TO WITHDRAW FROM A COURSE:
To be official, the class withdrawal must be in writing and signed by the student requesting the withdrawal; no withdrawal is accepted verbally. Please review the “Schedule of Classes”

(online or in-print) for procedures for class changes or withdrawals and the refund policy and schedule.

COURSE DELIVERY METHODOLOGY:
This course is delivered through Moodle. Students are expected to have reliable internet access, basic computer skills, the ability to upload/download files, use Amberton email, and submit assignments in the required format. Students needing assistance should use the Amberton SSO support/ticket process.

HOW TO ACCESS YOUR COURSE:

SINGLE SIGN-ON (SS0) INSTRUCTIONS FOR AMBERTON UNIVERSITY:
Students should access Amberton systems through the Single Sign-On portal at https://sso.amberton.edu. After logging in, students can access Moodle, Amberton email, CampusWeb, and other assigned applications. Students who need help accessing SSO should submit a support request through the SSO support option or contact support@amberton.edu..

MOODLE TUTORIAL:
Upon successful log in and access to the Moodle learning platform, there is a Student Moodle Tutorial course available, to learn about the basics of Moodle. Simply click on the link for the Student Moodle Tutorial and read through the various learning topics: Navigating; Communicating; Assignments & Exams; Grades; and Student Resources.

COURSE COMMUNICATIONS:
Students will communicate with faculty through the Moodle Learning Platform or the Amberton University email system.

EMAIL COMMUNICATION:
Students are expected to use their Amberton email account and Moodle for course communications. Students must use their official university email account for all university related communication and should check their Amberton emails regularly for course and university notices.

Upon completion of a session, all communication and course specific information is removed from the Moodle system. If a student needs to maintain a record of communications or assignments, the student is strongly encouraged to print out or download these items to a disk for their own records.

FORMAT AND SUBMISSION OF ASSIGNMENTS:
Assignments must be submitted through the appropriate Moodle assignment link unless otherwise directed by the instructor. Students are responsible for submitting files in the format required by the instructor.

INSTRUCTOR/COURSE EVALUATION:
Students will have the opportunity to complete an anonymous course and instructor evaluation near the end of the session. Instructions and dates will be provided through Moodle and/or Amberton email.

RESEARCH RESOURCES:
The Amberton Library provides access to full-text articles, peer-reviewed databases, and research tools, with options like Interlibrary Loan (ILL) and TexShare for items outside its collection. For research assistance, students can connect with library staff during operating hours via email (library@amberton.edu), phone (972-279-6511 ext. 185), "How-to" videos, live online chat, or in person at the Garland campus. The online library is available through Single Sign On (SSO).

MICROSOFT OFFICE 365 EDUCATION:
Amberton University students may access Microsoft 365 Education resources as provided by the university.

GOOGLE WORKSPACE FOR EDUCATION:
Amberton students are assigned a Google Workspace for Education account, including Amberton Gmail, Google Drive, Google Docs, Sheets, and Slides. Students should use their Amberton Google account for course-related work when required.