Syllabus for CYB-1200—Introduction to Cybersecurity

COURSE DESCRIPTION

Introduction to Cybersecurity provides an introductory study of cybersecurity terminology, principles, and technologies. Fundamental topics covered include cyber threats and vulnerabilities, information security frameworks, network infrastructure security, wireless network security, cryptography, defense-in-depth security strategy, information security policy, and security management. The goal is to develop a foundation for further study in cybersecurity.

COURSE TOPICS

- Fundamental concepts of cyber defense
    - CIA triad
    - Non-repudiation
    - Accountability
    - Laws/regulations
    - Defense-in-depth
    - Least privilege
    - Segregation of duties
    - Job rotation

- Identification of cyber defense tools
    - Methodology
    - Security mechanisms
    - Best practices
    - Vulnerability scans
    - IDS/IPS
    - SIEM solutions
    - Firewalls

- Technical and personnel-driven cyber threats
    - Advanced persistent threat (APT)
    - Insider threat
    - Script kiddies
    - Anonymous
    - Malware, DoS attacks, buffer overflows

- Symmetric and asymmetric algorithms used in encryption schemas
    - Symmetric encryption
    - Asymmetric encryption
    - PKI

- Implementation of secure architecture and infrastructures
    - Defense-in-depth/layered security
    - Data at rest and data in motion protections
    - Database and information security
    - DMZ

COURSE OBJECTIVES

After completing this course, you should be able to:

CO 1 Examine and identify threat agents and bad actors to networks including those involved in cyberterrorism and industrial espionage.

CO 2 Analyze defense-in-depth as it relates to layers of the OSI model.

CO 3 Interpret cyber defense concepts to determine practical implementation methods.

CO 4 Formulate and hypothesize how to implement tools and methods in defense of an attack.

CO 5 Analyze system compromise activities and mitigations.

CO 6 Scrutinize the first principles of network security including security risk assessment.

CO 7 Compare security mechanisms and determine how to implement them in a network.

CO 8 Compare and contrast symmetric and asymmetric algorithms used in encryption schemas.

CO 9 Analyze technologies and components used to defend networks against security issues to determine priority order in placement.

CO 10 Implement and utilize network monitoring tools.

COURSE MATERIALS

You will need the following materials to complete your coursework. Some course materials may be free, open source, or available from other providers. You can access free or open-source materials by clicking

the links provided below or in the module details documents. To purchase course materials, please visit the University's textbook supplier.

Required Textbook

- Easttom, W. (2023). *Computer security fundamentals* (5th ed.). Pearson IT Cybersecurity Curriculum (ITCC).
  ISBN-13: 978-0137984787

Note about Infosec Learning Labs: In completing your coursework, you will be using Infosec Learning Labs, a virtual platform that contains interactive labs that provide you with a real-world application and hands-on learning experience to practice various cybersecurity skills and concepts.

To access the labs, visit the Infosec section of the course website. When you click the Infosec Learning Labs link in your course for the first time, you will be redirected to an account setup page. You will be asked for some basic information to create your account and then make a payment. The price covers all labs needed for this course and access for six months.

COURSE STRUCTURE

Introduction to Cybersecurity is a three-credit, online course consisting of **six** modules. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

- **Module 1: Fundamental Concepts and Principles in Cybersecurity**
  Course objectives covered in this module: CO 2, CO 3, CO 4, CO 6

- **Module 2: Security Devices, Concepts, Principles, and Practices**
  Course objectives covered in this module: CO 4, CO 7, CO 9, CO 10

- **Module 3: Access, Network, and Physical Security Concerns**
  Course objectives covered in this module: CO 8, CO 9

- **Module 4: Incident Response**
  Course objectives covered in this module: CO 5, CO 10

- **Module 5: Business Continuity and Disaster Recovery**
  Course objective covered in this module: CO 9

- **Module 6: Threat Agents**
  Course objective covered in this module: CO 1

ASSESSMENT METHODS

For your formal work in the course, you are required to participate in online discussion forums, complete written assignments, complete Infosec Learning Labs, take quizzes, and complete a final project. See below for details.

Consult the Course Calendar for due dates.

Promoting Originality—One or more of your course activities may utilize a tool designed to promote original work and evaluate your submissions for plagiarism. More information about this tool is available in this document.

Discussion Forums

In addition to an ungraded Introductions Forum, you are required to participate in **six** graded online class discussions.

Communication with your mentor and among fellow students is a critical component of online learning. Participation in online class discussions involves two distinct activities: an initial response to a discussion question and at least two subsequent comments on classmates' responses.

All of these responses must be substantial. Meaningful participation is relevant to the content, adds value, and advances the discussion. Comments such as "I agree" and "ditto" are not considered value-adding participation. Therefore, when you agree or disagree with a classmate or your mentor, state and support your position.

You will be evaluated on the quality and quantity of your participation, including your use of relevant course information to support your point of view, and your awareness of and responses to the postings of your classmates. Remember, these are discussions: responses and comments should be properly proofread and edited, mature, and respectful. It is expected that you will use at least one APA-compliant reference (and corresponding in-text citations) for each initial post.

Written Assignments

You are required to complete **three** written assignments. The written assignments are on a variety of topics associated with the course modules. For specific details, consult the individual course modules.

Infosec Learning Labs

You are required to complete and submit results for **three** Infosec Learning Labs for this course. Each lab is either 90 minutes or 120 minutes in duration, regulated by a timer. They are designed to be completed in one sitting to simulate a real experience, so you cannot save your progress to return later. For an optimal experience, use a Chrome web browser with an Internet connection to run the labs.

While completing each lab, take a screenshot of the Lab Performance Report screen. **Submit both the screenshot and your lab reflection** to your mentor using the appropriate "Infosec Lab Results" link in Moodle.

The reflection questions consist of:

- What did you find difficult in the lab?
- What surprised you about the lab?
- What did you learn while doing the lab?
- How did the lab relate to the course topics? (Hint: you want to look at the learning objectives in the Syllabus).

Your mentor will review your submissions and give you credit for each completed activity. Be sure to reference the Course Calendar for due dates.

Please see the Infosec Learning Labs section of the course website for further details and instructions.

Quizzes

You are required to complete **six** quizzes for this course, one per individual module. All quiz items are multiple-choice and you may use course materials when taking the quizzes. There is no time limit for taking each quiz.

Most students find that quiz-taking is an excellent way to master the fundamental concepts, terms, and events related to the course content. Therefore, you will be able to take each quiz an unlimited number of times, and the gradebook will record your most recent score.

This arrangement will allow you to go back and reread portions of the text that you need to review and then take the quiz again for further practice.

Final Project

You are required to complete a final project, which includes a risk assessment report based on the themes discussed in this course. The main purpose of this project is to tie the concept of risk to a holistic

perspective of an organization's processes. Be sure to visit the Final Project area of the course website for full requirements, details, and instructions for this project. Consult the Course Calendar for due dates.

GRADING AND EVALUATION

Your grade in the course will be determined as follows:

- **Online discussions (6)**—20%
- **Written assignments (3)**—30%
- **Infosec Learning Labs (3)**—10%
- **Quizzes (6)**—10%
- **Final project (1)**—30%

All activities will receive a numerical grade of 0–100. You will receive a score of 0 for any work not submitted. Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	= 93–100	C+	= 78–79
A–	= 90–92	C	= 73–77
B+	= 88–89	C–	= 70–72
B	= 83–87	D	= 60–69
B–	= 80–82	F	= Below 60

To receive credit for the course, you must earn a letter grade of C or better (for an area of study course) or D or better (for a course not in your area of study), based on the weighted average of all assigned course work (e.g., exams, assignments, discussion postings).

STRATEGIES FOR SUCCESS

First Steps to Success

To succeed in this course, take the following first steps:

- Read carefully the entire Syllabus, making sure that all aspects of the course are clear to you and that you have all the materials required for the course.

- Take time to read the entire Online Student Handbook. The Handbook answers many questions about how to proceed through the course, and how to get the most from your educational experience at Thomas Edison State University.

- Familiarize yourself with the learning management systems environment—how to navigate it and what the various course areas contain. If you know what to expect as you navigate the course,

you can better pace yourself and complete the work on time.

- If you are not familiar with web-based learning, be sure to review the processes for posting responses online and submitting assignments before class begins.

Study Tips

Consider the following study tips for success:

- To stay on track throughout the course, begin each week by consulting the Course Calendar. The Course Calendar provides an overview of the course and indicates due dates for submitting assignments, posting discussions, and submitting the final project.

- Check Announcements regularly for new course information.

Using AI Ethically: A Guide for TESU Students

TESU's Academic Code of Conduct permits student AI use in support of their writing and research process--not as a replacement for original writing. Document AI use with an acknowledgment statement at the end of each assignment, noting the tools and prompts used. Cite any AI-generated content on the References page. Please review Using AI Ethically: A Guide for TESU Students for more detailed information.

COMMITMENT TO DIVERSITY, EQUITY, AND INCLUSION

Thomas Edison State University recognizes, values, and relies upon the diversity of our community. We strive to provide equitable, inclusive learning experiences that embrace our students' backgrounds, identities, experiences, abilities, and expertise.

ACCESSIBILITY AND ACCOMMODATIONS

Thomas Edison State University adheres to the Americans with Disabilities Act (ADA, 1990; ADAAA, 2008) and Section 504 of the Rehabilitation Act of 1973. The Office of Student Accessibility Services (OSAS) oversees requests for academic accommodations related to disabilities; a student who is pregnant, postpartum, or a student parenting a newborn who is not the birth parent [as covered under NJSA18A]; and students requesting academic accommodation for a short-term/temporary illness and/or injury. Information can be found on the Office of Student Accessibility Services webpage and questions can be sent to ADA@tesu.edu.

ACADEMIC POLICIES

To ensure success in all your academic endeavors and coursework at Thomas Edison State University, familiarize yourself with all administrative and academic policies including those related to academic integrity, course late submissions, course extensions, and grading policies.

For more, see:

- University-wide policies
- Undergraduate academic policies
- Undergraduate course policies
- Graduate academic policies
- Graduate course policies
- Nursing student policies
- Nursing graduate student policies
- International student policies
- Academic code of conduct