

Information Technology Security (ITSY 1342) Online



Credit: 3 semester credit hours (2 hours lecture, 4 hours lab)

Prerequisite/Co-requisite: Completed the [Online Orientation](#) and answered Yes to 7+ questions on the Online Learner Self-Evaluation:
<https://www.lit.edu/Online-Learning/Online-Orientation/Is-Distance-Learning-Right-for-Me/Self-Evaluation/>.

Course Description

Instruction in security for network hardware, software, and data, including physical security: backup procedures: relevant tools: encryption: and protection from viruses. *This course is time-bound, structured, and completed online.*

Required Textbook and Materials

1. Cengage MindTap access to **CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition, Ciampa, Mark; Cengage, 2022**
 - a. **How to buy your Course Materials**
 - Step 1: Sign into **Blackboard** and click on **this course**
 - Step 2: Click on the Cengage link: **Getting Started** in the *Getting Started with Cengage MindTap* section.
 - Step 3: Create or sign into your Cengage account to access or purchase the materials for this course.

NOTE: If you are taking additional courses that use Cengage materials, you can save by purchasing a Cengage Unlimited plan, which gives you access to all Cengage eTextbooks and online homework platforms for one price. Visit cengage.com/unlimited or your campus bookstore to learn more.
 - b. Beware of sites that are selling discounted codes. These sources are likely unauthorized sellers who have acquired access codes illegally, and transactions with such sources may pose a risk to your personal information.
 - c. Need help? Visit startstrong.cengage.com for step-by-step registration instructions and videos.
2. Computer with internet access.
3. Computer Networking and Troubleshooting Technology and Cyber Security students are required to have one 64 GB or larger capacity USB Flash Drive to be used for the duration of the time to complete their respective degree.

Course Objectives

Upon completion of this course, the student will be able to:

1. Employ the physical security of network infrastructure components using National Institute of Standards and Technology (NIST) Guidelines and other best practices.
2. Develop backup procedures to provide for data security.
3. Use network operating system features to implement network security.
4. Identify computer and network threats and vulnerabilities and methods to prevent their effects.
5. Use tools to enhance network security.
6. Use encryption techniques to protect network data.

Course Outline

Part 1: Security Fundamentals

1. Introduction to Security
2. Threat Management and Cybersecurity Resources

Part 2: Endpoint Security

3. Threats and Attacks on Endpoints
4. Endpoint and Application Development Security
5. Mobile, Embedded, and Specialized Device Security

Part 3: Cryptography

6. Basic Cryptography
7. Public Key Infrastructure and Cryptographic Protocols

Part 4: Network Security

8. Networking Threats, Assessments, and Defenses
9. Network Security Appliances and Technologies
10. Cloud and Virtualization Security
11. Wireless Network Security

Part 5: Enterprise Security

12. Authentication
13. Incident Preparation, Response, and Investigation
14. Cybersecurity Resilience
15. Risk Management and Data Privacy

Grade Scale

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
0 – 59	F

Course Evaluation

Final grades will be calculated according to the following criteria:

Discussion Posts	5%
Labs	25%
Study Guides	10%
Tests	30%
Final Exam	30%

Course Requirements

1. Demonstrate proficiency through hands-on labs as assigned.
2. Complete Study Guides and worksheets as assigned.
3. Students can complete this course without physically visiting the institution offering the course.
4. The student will post discussions as instructed along with any other assignments instructed to complete.

Course Policies

1. You must log onto Blackboard and access this course a minimum of three times per week.
2. Certification: If a student passes the certification test that is associated with this class, you will receive an “A” on the final exam and credit for 25% of your labs. If you have missed a previous test, you must still take the final exam to substitute for that grade.
3. If you wish to drop a course, the student is responsible for initiating and completing the drop process. If you stop coming to class and fail to drop the course, you will earn an ‘F’ in the course.
4. A grade of ‘C’ or better must be earned in this course for credit toward degree requirement.
5. Internet Usage – Students are expected to use proper net etiquette while participating in course emails, assignment submissions, and online discussions.
6. Additional course policies, as defined by the individual course instructor, will be outlined in the course addendum and provided by the instructor.

Technical Requirements

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at:

https://help.blackboard.com/Learn/Student/Getting_Started/Browser_Support/Browser_Checker.

A functional internet connection, such as DSL, cable, or WiFi is necessary to maximize the use of the online technology and resources.

Disabilities Statement

The Americans with Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973 are federal anti-discrimination statutes that provide comprehensive civil rights for persons with disabilities. LIT provides reasonable accommodations as defined in the Rehabilitation Act of 1973, Section 504 and the Americans with Disabilities Act of 1990, to students with a diagnosed disability. The Special Populations Office is located in the Eagles’ Nest Room 129 and helps foster a supportive and inclusive educational environment by maintaining partnerships with faculty and staff, as well as promoting

awareness among all members of the Lamar Institute of Technology community. If you believe you have a disability requiring an accommodation, please contact the Special Populations Coordinator at (409) 839-2018. You may also visit the online resource at [Special Populations - Lamar Institute of Technology \(lit.edu\)](http://Special Populations - Lamar Institute of Technology (lit.edu)).

Starfish

LIT utilizes an early alert system called Starfish. Throughout the semester, you may receive emails from Starfish regarding your course grades, attendance, or academic performance. Faculty members record student attendance, raise flags and kudos to express concern or give praise, and you can make an appointment with faculty and staff, all through the Starfish home page. You can also log in to Blackboard or MyLIT and click on the Starfish link to view academic alerts and detailed information. It is the responsibility of the student to pay attention to these emails and information in Starfish and consider taking the recommended actions. Starfish is used to help you be a successful student at LIT. For more information, visit <https://lit.edu/student-success/starfish>.

Student Code of Conduct Statement

It is the responsibility of all registered Lamar Institute of Technology students to access, read, understand and abide by all published policies, regulations, and procedures listed in the *LIT Catalog and Student Handbook*. The *LIT Catalog and Student Handbook* may be accessed at www.lit.edu or obtained in print upon request at the Student Services Office. Please note that the online version of the *LIT Catalog and Student Handbook* supersedes all other versions of the same document.

Certification Requirement

CNTT and Cyber Security majors are required to earn certification in one of the following areas prior to graduation.

- A+ Certification
- Network+ Certification
- Security+ Certification
- Linux+ Certification
- Cisco Certified Network Associate (CCNA)

This course covers the material to prepare for CompTIA's Security+ certification, exam number SY0-601. If taken, students are responsible for scheduling and paying for the certification through the LIT Testing Center for online testing, if available. More information about the certification can be found online at <https://www.comptia.org/certifications/security>.