CƠ SỞ AN TOÀN THÔNG TIN (FUNDAMENTALS OF INFORMATION SECURITY)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: Cơ sở an toàn thông tin (Fundamentals of Information Security)

Course code: SEC1401_CLC

Course type: Compulsory

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with the basic knowledge about information security and and information systems security.

Skills:

On successful completion of this course a student will be able to:

- analyze security threats and risks to information and information systems;
- deploy appropriate security techniques and tools to solve common problems in information security.

Attitude:

Students are required to attend the classes and complete assignments/projects.

3. Abstracts

This course provides students with basic knowledge about information security and information systems security, including security requirements, general protection model of information systems, security threats, common computer/network attacks and malwares; Techniques and technologies to secure information and systems, such as information security based on cryptographic techniques, access control and user authentication, firewalls, intrusion detection and prevention systems; Information security management, laws and policies.

4. Teaching and learning methods

Lectures:	24h
Exercises:	5h
Projects:	8h
Labs:	8h
Individual reading:	0h

5. Prerequisites: Computer Networks - INT1336_CLC

6. Learning outcomes

After completing this course, the student is able to:

[CLO1]: Explain the basic knowledge, ethical issues and professional responsibility in information security field;
[CLO2]: Analyze security threats and risks to information and information systems
[CLO3]: Deploy appropriate security techniques and tools to solve common problems in information security.

7. Assignment criteria

Learning outcomes	**Assignment criteria**
[CLO1]: Explain the basic knowledge, ethical issues and professional responsibility in information security field	Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5, Chapter 6
[CLO2]: Analyze security threats and risks to information and information systems	Chapter 2, Chapter 3
[CLO3]: Deploy appropriate security techniques and tools to solve common problems in information security	Chapter 4, Chapter 5, Chapter 6

8. Outlines

Chapter 1 Introduction to information security

1.1. Overview of information security
    1.1.1. What is information security?
    1.1.2. Components of information security
1.2. Overview of information systems security
    1.2.1. Components of an information system
    1.2.2. What is information systems security?
1.3. Requirements of information systems security
    1.3.1. Confidentiality
    1.3.2. Integrity
    1.3.3. Availability
1.4. Areas of information technology infrastructure and security threats
    1.4.1. Sven areas of information technology infrastructure
    1.4.2. Security threats
1.5. General model for information systems security
    1.5.1. Defense in Depth model
    1.5.2. Protection layers of Defense in Depth model

Chapter 2 System weaknesses and vulnerabilities

2.1. Introduction to system weaknesses and vulnerabilities
2.2. Common vulnerabilities in operating systems and software applications
2.3. Manage, fix security vulnerabilities and enhance system resilience
2.4. Introduction to scanning tools for vulnerabilities and security vulnerabilities

Chapter 3 Common Attacks and Malwares

3.1. Introduction to security threats and attacks
    3.1.2. Types of common security threats

3.1.4. Types of attacks
3.2. Attacking support tools
3.2.1. Weakness and vulnerability scanners
3.2.2. Service port scanners
3.2.3. Sniffing tools
3.2.4. Key-loggers
3.3. Common computer and network attacks
3.3.1. Overview
3.3.2. Common attacks
3.4. Common computer and network malwares
3.4.1. Overview
3.4.2. Common malwares

Chapter 4 Cryptographic Techniques for Information Security

4.1. Introduction to cryptography and its applications
4.1.1. Common concepts
4.1.2. Elements of a cryptosystem
4.1.3. History of cryptography
4.1.4. Stream ciphers and block ciphers
4.1.5. Applications of cryptography
4.2. Traditional cryptographic methods
4.3. Modern cryptographic algorithms
4.3.1. Symmetric key ciphers
4.3.2. Asymmetric key ciphers
4.3.3. Hash functions

Chapter 5 Techniques and Technologies for Information Security

5.1. Overview of techniques and technologies for information security
5.2. Access control
5.2.1. Overview
5.2.2. Access control models
5.2.3. Access control technologies
5.3. Firewalls
5.4. IDS and IPS
5.4.1. Overview
5.4.2. IDS/IPS classification
5.4.3. Intrusion detection techniques
5.5. Anti-malware tools

Chapter 6 Information security management, laws and policies

6.1. Information security management
6.1.1. Overview
6.1.2. Risk assessment
6.1.3. Detailed risk analysis
6.1.4. Implementation of information security management
6.2. Information security management standards
6.3. Laws and Policies in information security
6.3.1. Overview of information security laws and policies

6.3.2. International information security laws
6.3.3. Vietnamese information security laws
6.4. Ethics in information security

9. Required Textbooks

[1] Michael E. Whitman, Herbert J. Mattord, *Principles of information security*, 7th edition, Course Technology, Cengage Learning, 2021.
[2] David Kim, Michael G. Solomon, *Fundamentals of Information Systems Security*, 3th edition, Jones & Bartlett Learning, 2016.

10. Suggested Textbooks

[3] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996.
[4] Hoàng Xuân Dậu, *Giáo trình cơ sở an toàn thông tin*, Học viện Công nghệ BCVT, NXB Thông tin & Truyền thông, 2020.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1 Introduction to information security	3h lecture	1.1. Overview of information security 1.2. Overview of information systems security 1.3. Requirements of information systems security 1.4. Areas of information technology infrastructure and security threats 1.5. General model for information systems security
Chapter 2 System weaknesses and vulnerabilities	4h lecture 1h exercise	2.1. Introduction to system weaknesses and vulnerabilities 2.2. Common vulnerabilities in operating systems and software applications 2.3. Manage, fix security vulnerabilities and enhance system resilience 2.4. Introduction to scanning tools for vulnerabilities and security vulnerabilities
Chapter 3 Common Attacks and Malwares	5h lecture 2h exercise 3h project 3h lab	3.1. Introduction to security threats and attacks 3.2. Attacking support tools 3.3. Common computer and network attacks 3.4. Common computer and network malwares
Chapter 4 Cryptographic	5h lecture 1h exercise 3h project	4.1. Introduction to cryptography and its applications 4.2. Traditional cryptographic methods 4.3. Modern cryptographic algorithms

Techniques for Information Security	3h lab	
Chapter 5 Techniques and Technologies for Information Security	4h lecture 1h exercise 2h project 2h lab	5.1. Overview of techniques and technologies for information security 5.2. Access control 5.3. Firewalls 5.4. IDS and IPS 5.5. Anti-malware tools
Chapter 6 Information security management, laws and policies	3h lecture	6.1. Information security management 6.2. Information security management standards 6.3. Laws and Policies in information security 6.4. Ethics in information security

12. Grading Policy

Attendance:	10%
Mid-term exam/exercises:	10%
Course projects:	30%
Final examination:	50%