

# FUNDAMENTALS OF INFORMATION SECURITY

## 1. Thông tin về học phần (General Information)

**Tên học phần (Course name):** Fundamentals of Information Security

**Mã học phần (Course code):** INT1472

**Số tín chỉ (Number of credits):** 3

**Loại học phần (Course type):** Compulsory

**Học phần tiên quyết (Prerequisites):**

**Học phần trước (Previous courses):** Computer Networks (INT1336)

**Học phần song hành (Parallel courses):**

**Các yêu cầu đối với học phần (Course requirements):**

- Lecture room: Projector, microphone and speaker.
- Laboratory: LAN computers with internet connection.

**Giờ tín chỉ đối với các hoạt động (Teaching and Learning hours):**

- Lý thuyết (Lectures): 30h
- Bài tập (Exercises): 0h
- Bài tập lớn (Projects): 8h
- Thực hành (Labs): 7h
- Tự học (Individual reading): 0h

**Địa chỉ Khoa/Bộ môn phụ trách học phần (Address of the Faculty/Department in charge of the course):**

- Address: Faculty of Information Technology 1 - Posts and Telecommunications Institute of Technology, Km10, Nguyen Trai Street, Ha Dong District, Hanoi.
- Phone number: (024) 33510432

## 2. Mục tiêu học phần (Objectives)

**Về kiến thức (Knowledge):**

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

- security requirements, general security model, security threats, common computer/network attacks and malwares;
- techniques and technologies to secure information and systems;
- information security management, laws and policies.

**Kỹ năng (Skills):**

The aim of this course is to equip students with skills in:

- analyzing of security threats and risks to information and information systems;
- selecting suitable security measures to protect information and information systems in practice.

**Thái độ, Chuyên cần (Attitude):**

Students must ensure the required class attendance, assigned projects & labs and self-studying hours.

### **3. Tóm tắt nội dung học phần (Description)**

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. Nội dung chi tiết học phần (Outlines)**

#### **Chapter 1 Introduction**

- 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 Common Attacks and Malwares**

- 2.1. Introduction to security threats, weaknesses, vulnerabilities and attacks
  - 2.1.1. Concepts of security threats, weaknesses, vulnerabilities and attacks
  - 2.1.2. Types of common security threats
  - 2.1.3. Common vulnerabilities in operating systems and software applications
  - 2.1.4. Types of attacks
- 2.2. Attacking support tools
  - 2.2.1. Weakness and vulnerability scanners
  - 2.2.2. Service port scanners
  - 2.2.3. Sniffing tools
  - 2.2.4. Key-loggers
- 2.3. Common computer and network attacks
  - 2.3.1. Overview
  - 2.3.2. Common attacks
- 2.4. Common computer and network malwares
  - 2.4.1. Overview
  - 2.4.2. Common malwares

#### **Chapter 3 Cryptographic Techniques for Information Security**

- 3.1. Introduction to cryptography and its applications
  - 3.1.1. Common concepts
  - 3.1.2. Elements of a cryptosystem
  - 3.1.3. History of cryptography
  - 3.1.4. Stream ciphers and block ciphers

- 3.1.5. Applications of cryptography
- 3.2. Cryptographic methods
- 3.3. Cryptographic algorithms
  - 3.3.1. Symmetric key ciphers
  - 3.3.2. Asymmetric key ciphers
  - 3.3.3. Hash functions
- 3.4. Digital signatures, public key certificates and PKI
  - 3.4.1. Digital signatures
  - 3.4.2. Public key certificates
  - 3.4.3. PKI
- 3.5. Key management and key distribution
  - 3.5.1. Overview
  - 3.5.2. Secret key distribution
  - 3.5.3. Public key distribution
- 3.6. Secure communication protocols based on cryptographic techniques
  - 3.6.1. SSL/TLS
  - 3.6.2. SET
  - 3.6.3. PGP

## **Chapter 4 Techniques and Technologies for Information Security**

- 4.1. Access control
  - 4.1.1. Overview
  - 4.1.2. Access control models
  - 4.1.3. Access control technologies
- 4.2. Firewalls
- 4.3. IDS and IPS
  - 4.3.1. Overview
  - 4.3.2. IDS/IPS classification
  - 4.3.3. Intrusion detection techniques
- 4.4. Anti-malware tools

## **Chapter 5 Information security management, laws and policies**

- 5.1. Information security management
  - 5.1.1. Overview
  - 5.1.2. Risk assessment
  - 5.1.3. Detailed risk analysis
  - 5.1.4. Implementation of information security management
- 5.2. Information security management standards
- 5.3. Laws and Policies in information security
  - 5.3.1. Overview of information security laws and policies
  - 5.3.2. International information security laws
  - 5.3.3. Vietnamese information security laws
- 5.4. Ethics in information security

## **5. Học liệu (Textbooks)**

### **5.1. Học liệu bắt buộc (Required Textbooks)**

- [1] Michael E. Whitman, Herbert J. Mattord, Principles of information security, 4th edition, Course Technology, Cengage Learning, 2012.
- [2] David Kim, Michael G. Solomon, Fundamentals of Information Systems Security, Jones & Bartlett learning, 2012.

### **5.2. Học liệu tham khảo (Optional Textbooks)**

- [3] Hoàng Xuân Dâu, Bài giảng An toàn bảo mật hệ thống thông tin, Học viện Công nghệ Bưu chính viễn thông, 2017.

[4] Matt Bishop, Introduction to Computer Security, Prentice Hall, 2004.

[5] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.

## 6. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập học phần (Grading Policy)

| <b>Grading method</b> | <b>Percentage</b> | <b>Group/Individual</b> |
|-----------------------|-------------------|-------------------------|
| - Attendance          | 10%               | Individual              |
| - Mid-term exams      | 10%               | Individual              |
| - Projects            | 20%               | Group or individual     |
| - Final examination   | 60%               | Individual              |

**Trưởng Bộ môn**  
**(Head of Department)**

**Giảng viên biên soạn**  
**(Lecturer)**

**Hoàng Xuân Dậu**

**Hoàng Xuân Dậu**