Course Syllabus

1. **Program of Study** Bachelor of Business Administration Program
   Faculty/Institute/College Mahidol University International College

2. **Course Code** ICIS 387
   Course Title Information Systems Security

3. **Number of Credits** 4 **(Lecture/Lab)** (4-0-8)

4. **Prerequisite(s)** -

5. **Type of Course** Elective Course

6. **Trimester / Academic Year** Second Trimester/2007-2008

7. **Course Conditions** 20-40 students

8. **Course Description**
   Examines potential security risks in today's intensive information organizations. Topics that would be covered include viruses, security reviews, encryption, authentication, firewalls, and disaster recovery plans.

9. **Course Objective(s)**
   After successful completion of this course, students will be able to
   - 9.1 Able to understand the risks associated with computer security.
   - 9.2 Understand the different types of security threats and be able to analyze and solve problems effecting organizations.
   - 9.3 Define an information security strategy and architecture.

10. Course Outline

Week	Course Outline				Instructor
	Topics	**Lecture**	**Lab**	**Self-Study**	
1	Introduction to Information Security	4	0	8	VRB
2	Why Security? Threats and Attacks	4	0	8	VRB
3	Legal, Ethical & Professional Issues	4	0	8	VRB
4	Security Policy	4	0	8	VRB
5	Security Technologies	4	0	8	VRB
6	Disaster Recovery & Business Continuity	4	0	8	VRB
7	Physical Security	4	0	8	VRB
8	Implementing Security	4	0	8	VRB
9	Computer & Network Security Workshop	4	0	8	VRB
10	The Human Factor in Information Security	4	0	8	VRB
11	Information Security as an Ongoing Effort	4	0	8	VRB
	Total	**44**	**0**	**88**	

11. Teaching Method(s)

All materials will be covered by lecturing during the class time.
Examples and case studies will be discussed through question-answer time.
In-class quizzes.

12. Teaching Media

N/A

13. Measurement and Evaluation of Student Achievement

Students achievement is measured and evaluated by

13.1 The ability to understand the risks associated with computer security.

13.2 The ability to understand the different types of security threats and be able to analyze and solve problems effecting organizations.

13.3 The ability to define an information security strategy and architecture.

Student's achievement will be graded according to the faculty and university standard using the symbols: A, B+, B, C+, C, D+, D, and F.

Student must have attended at least 80% of the total class hours of this course.

Ratio of mark	
1. Midterm	45%
2. Final	45%
3. Quizzes	10%

14. Course Evaluation

14.1 Students' achievement as indicated in number 13 above.

14.2 Students' satisfaction towards teaching and learning of the course using questionnaires.

15. Reference(s)

Whitman & Mattord (2004). **Management of Information Security.** Thomson Course Technology. ISBN: 0-619-21515-1

16. Instructor(s)

Veera Bhatiasevi

17. Course Coordinator

Program Director of Information Systems Major