City University of Hong Kong
Course Syllabus

offered by Department of Computer Science
with effect from Semester A 2017/18

Part I Course Overview

Course Title:	Information Security Technology Management
Course Code:	CS5294
Course Duration:	One semester
Credit Units:	3 credits
Level:	P5
Medium of Instruction:	English
Medium of Assessment:	English
Prerequisites: *(Course Code and Title)*	Nil
Precursors: *(Course Code and Title)*	Nil
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

The course provides an overview of the concepts and elements in information security technology management. It is important that information security requirements be understood at the organizational level; appropriate information security policy be derived; cost-effective information security solution be planned and deployed; and evidence to auditors be provided on how well an organization has performed when required.

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs	Weighting (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Describe major information security technologies; understand their limitations and applications as countermeasures to IT threats.			✓	
2.	Describe threats and vulnerabilities in an IT environment; and recognize the relationship of threat, vulnerability, and countermeasure; and its impact on organizational information security.			✓	
3.	Describe the information security management framework; formulate a basic information security policy for an organization and design appropriate guidelines in implementing the policy with reference to appropriate Information Security Management Standards.		✓	✓	
4.	Recognize and critique legal issues in information security.		✓		
		100%			

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to self-life problems.

A3: *Accomplishments*
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

Teaching pattern:
Suggested lecture/tutorial/laboratory mix: 2 hrs. lecture; 1 hr. tutorial.

TLA	Brief Description	CILO No.				Hours/week (if applicable)
		1	2	3	4	
Lectures	Lectures to introduce the basic concepts, the relationship of these concepts and their practical use in information security technology management.	✓	✓	✓	✓	2 hours/ week
Tutorials	Tutorial sessions used for understanding the concepts related to the lectures and discussing some real life examples in applying the concepts.	✓	✓	✓	✓	1 hour/ week
Group assignment 1 – simple risk analysis	Students are required to identify threats, vulnerabilities, and countermeasures in a given security scenario, and inquire on their effectiveness.	✓	✓			2 hours/ week for 4 weeks
Group assignment 2 – simple policy statement with solutions	Students are required to design simple information security policy, to recommend controls according to standards, to suggest associated guidelines for recommended controls and to suggest some audit questions.		✓	✓		2 hours/ week for 4 weeks

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

Assessment Tasks/Activities	CILO No.				Weighting	Remarks
	1	2	3	4		
Continuous Assessment: 30%						
Group assignment 1	✓	✓			12%	
Group assignment 2		✓	✓		12%	
Short test	✓				6%	
Examination^: 70% (duration: 2 hours)						
					100%	

^ For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
1. Assignment 1	Ability to identify Threats and Vulnerabilities in Scenarios	High	Significant	Moderate	Basic	Below marginal level
	Ability to understand the relationship among Threats, Vulnerabilities and Countermeasures	High	Significant	Moderate	Basic	Below marginal level
2. Assignment 2	Ability to write simple but high level information security objectives in a given IT environment with controls proposed based upon a given standard	High	Significant	Moderate	Basic	Below marginal level
	Ability to propose reasonable procedures/ guidelines matching the security objectives based upon a given standard	High	Significant	Moderate	Basic	Below marginal level
	Ability to suggest checklist /questions from the perspective of security auditing matching the security objectives based upon a given standard	High	Significant	Moderate	Basic	Below marginal level
3. Short Test	Ability to explain and apply information security technologies as security countermeasures	High	Significant	Moderate	Basic	Below marginal level

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

(An indication of the key topics of the course.)

Information security: risks and attacks, organizational requirements; information security management: policy, risk assessment, business continuity planning, information security management standards and compliance; legal issues: computer crimes and forensics; information security audits; related technologies and tools.

Syllabus

1. Overview of Information security
   - Risks and attacks in an information system environment.
   - Requirements on confidentiality, integrity, availability, authentication, non-repudiation

2. Information Security Technologies
   - Access control
     Network security problems, access control methods, firewalls, physical access control, computer access control models, mandatory and discretionary policies, operating system access control
   - Encryption techniques
     Confidentiality solutions, symmetric encryption, AES, public key encryption, RSA, key management
   - Authentication and Public key Infrastructure
     Authentication techniques: password, cryptography, biometric; authentication protocols, digital signature, trust models, digital certificates, Certificate Authority, revocation

3. Information Security Management
   - Security policies, relationship to business process
   - Security organizations
   - Risk analysis processes
   - Information Security Management Standards

4. Legal Issues
   - Cyber Crimes
   - E-commerce law
   - Data protection issues
   - Compliance and Information Security Audits

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

1.	Whitman and Mattord (2010). *Management of Information Security*, Cengage Learning, 4th edition.

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

1.	Merkow & Breithaupt (2005), Information Security: Principles and Practices, Pearson
2.	Greene (2006), Security Polices and Procedures: Principles and Practices, Pearson