City University of Hong Kong
Course Syllabus

offered by Department of Information Systems
with effect from Semester A in 2017 / 2018

Part I Course Overview

Course Title:	Cybersecurity for Business
Course Code:	IS3501
Course Duration:	One Semester (13 Weeks)
Credit Units:	3
Level:	B3
Proposed Area: *(for GE courses only)*	☐ Arts and Humanities ☐ Study of Societies, Social and Business Organisations ☐ Science and Technology
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

(A 150-word description about the course)

Internet is part of our life today and Cybersecurity is becoming extremely important for Internet. This course aims to provide students with an overview of information security knowledge so as to protect an organization's information assets. Upon completion of this course, students are able to make use of privacy and security management models in today's dynamic business environment. Moreover, students can learn how to apply security knowledge for various business applications.

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 the concept and key elements in data communication and information security.	25%	✓	✓	
2.	Assess the value of information asset and the threats in today's business environment.	25%	✓		✓
3.	Demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.	20%		✓	✓
4.	Assess the impacts of the proposed security management solution on the operation of organisations.	15%		✓	✓
5.	Exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.	15%		✓	✓
** If weighting is assigned to CILOs, they should add up to 100%.*		100%			

[#] Please specify the alignment of CILOs to the Gateway Education Programme Intended Learning outcomes (PILOs) in Section A of Annex.

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.)

TLA	Brief Description	CILO No.					Hours/week (if applicable)
		1	2	3	4	5	
TLA1: Lecture	The following items form the content of the lecture: o Security Management Policies & Practices: Identification of information assets and development, documentation, implementation of policies, standards, procedures and guidelines, ethics and legal issues. o Basics of Data Communication: Concepts related to fundamentals of data communication and networking, different types of networks and communication services and network management. o Security Architecture and Models: Concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment networks, applications and those controls used to enforce various levels of availability, integrity and confidentiality. o Access Control Systems and Methodology: Collection of mechanisms that work together to create security architecture to protect assets of the information systems. o Cryptography: Principles, means, methods of disguising information to ensure its integrity, confidentiality and authenticity.	✓	✓	✓	✓	✓	2 hrs/wk
TLA2: Case Studies	Students will be required to work on case studies associated with different aspects of information security management. For each case study, students will carry out analysis and formulate recommendations for appropriate security solutions.	✓	✓	✓	✓	✓	1 hr/wk
TLA3: Group Presentation	All students will be required to work in a small group on one of the topics covered in the lecture. They are expected to provide background information, present their critical assessment on particular security problem and make recommendations of how organisation resolve this problem with good security management practices.	✓	✓	✓	✓	✓	

4. Assessment Tasks/Activities (ATs)

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

Indicative of likely activities and tasks students will undertake to learn in this course. Final details will be provided to students in their first week of attendance in this course.

Assessment Tasks/Activities	CILO No.					Weighting *	Remarks[#]
	1	2	3	4	5		
Continuous Assessment: 50%							
AT1: Tutorial Participation Each tutorial consists of exercises, small group discussions, self-reflection, or student presentations to assess students' understanding of the chosen topics and their abilities to apply their skills.	✓	✓	✓	✓	✓	20%	
AT2: Group Project A group project, which includes a project report and presentation, will be allocated to let students apply security management concepts and methodology to solve security risks in the organisation.	✓	✓	✓	✓	✓	30%	
Examination: 50% (duration: one 2-hour exam)							
AT3: Examination A written examination is developed to assess student's competence level of the taught subjects.	✓	✓	✓	✓	✓	50%	
** The weightings should add up to 100%.*						100%	

[#] Remark: Students must pass BOTH coursework and examination in order to get an overall pass in this course.

5. Assessment Rubrics

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

Assessment Task (AT)	**Criterion**	**Excellent (A+, A, A-)**	**Good (B+, B, B-)**	**Fair (C+, C, C-)**	**Marginal (D)**	**Failure (F)**
AT1: Tutorial Participation	Ability to describe the concept and key elements in data communication and information security.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to assess the value of information asset and the threats in today's business environment.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to assess the impacts of the proposed security management solution on the operation of organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to exercise good communication and interpersonal skills in	High	Significant	Moderate	Basic	Not even reaching marginal

	proposing and presenting appropriate security management framework.					levels
AT2: Group Project	Ability to describe the concept and key elements in data communication and information security.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to assess the value of information asset and the threats in today's business environment.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to assess the impacts of the proposed security management solution on the operation of organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.	High	Significant	Moderate	Basic	Not even reaching marginal levels
AT3: Examination	Ability to describe the concept and key elements in data communication and information security.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to assess the value of information asset and the threats in today's business environment.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to demonstrate consultative problem solving skills by creatively and innovatively selecting and applying most security management approaches for modern organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Capability to assess the impacts of the proposed security management solution on the operation of organisations.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Ability to exercise good communication and interpersonal skills in proposing and presenting appropriate security management framework.	High	Significant	Moderate	Basic	Not even reaching marginal levels

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.)

Privacy and security policies; Security management; Access controls; Data security; Internet security; Ethical and legal issues in cybersecurity.

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.	Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger Davis, Dwayne Williams, Principles of Computer Security, McGraw-Hill Education; 4 edition (December 29, 2015).

2.2 Additional Readings

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

1.	William Stallings, Lawrie Brown, Computer Security, 2/E, Pearson, 2012, ISBN: 978-0-13-277506-9.
2.	Randall J. Bolyle, Raymond R. Panko, Corporate Computer Security, 4/E, 2015, Pearson, ISBN: 978-0-13-354519-7.
3.	Harold F. Tipton, Micki Krause Nozaki, Information Security Management Handbook, Auerbach Publications, 6 edition (November 2, 2016).