***Form 2B***

# City University of Hong Kong

## Information on a Course
**offered by Department of Computer Science**
**with effect from Semester A in 2012 / 2013**

---

**Part I**

**Course Title**: Information Security Technology Management

**Course Code**: CS5294

**Course Duration**: One Semester

**Credit Units**: 3

**Level**: P5

**Medium of Instruction**: English

**Prerequisites**: Nil

**Precursors**: Nil

**Equivalent Courses**: Nil

**Exclusive Courses**: Nil

**Part II**

**Course Aims**

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.

**Course Intended Learning Outcomes (CILOs)**
*Upon successful completion of this course, students should be able to:*

| No. | CILOs | Weighting (if applicable) |
|---|---|---|
| 1. | describe threats in IT environment; and recognize and inquire the relationship of threat, vulnerability, | |

| | | |
|---|---|---|
| | countermeasure, and impact in organizational information security; | |
| 2. | formulate basic information security policy for an organization and design appropriate guidelines in implementing the policy; | |
| 3. | describe the information security management framework and the roles of Information Security Management Standards in this framework; | |
| 4. | recognize and critique legal issues in information security. | |

## Teaching and Learning Activities (TLAs)

*(Indicative of likely activities and tasks designed to facilitate students' achievement of the CILOs. Final details will be provided to students in their first week of attendance in this course)*

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

| **CILO No.** | **TLAs** | **Hours/week (if applicable)** |
|---|---|---|
| CILO 1-4 | Lectures to introduce the basic concepts, the relationship of these concepts and their practical use in information security technology management. | 2 hours/ week |
| CILO 1-4 | Tutorial sessions used for understanding the concepts related to the lectures and discussing some real life examples in applying the concepts. | 1 hour/ week |

## Assessment Tasks/Activities

*(Indicative of likely activities and tasks designed to assess how well the students achieve the CILOs. Final details will be provided to students in their first week of attendance in this course)*

| **CILO No.** | **Type of Assessment Tasks/Activities** | **Weighting (if applicable)** | **Remarks** |
|---|---|---|---|
| CILO 1 | **Coursework:** Students are required to identify threats, vulnerabilities, and countermeasures in a given security scenario, and inquire on their effectiveness.<br>**Examination:** Questions assessing understanding of basic information security technologies, threats, vulnerabilities and their relationship. | | |
| CILO 2 | **Coursework:** Students are required to design simple information security policy, | | |

| | | | |
|---|---|---|---|
| | and its associated guidelines.<br>**Examination:** Questions assessing understanding of concepts and contents in an information security policy. | | |
| CILO 3 | **Examination:** Questions assessing understanding of importance of the standard and how standards are used in planning and auditing of information security in an organization. | | |
| CILO 4 | **Examination:** Questions assessing understanding of issues and principles of related legal aspects related to information security. | | |

**Grading of Student Achievement:** Refer to Grading of Courses in the Academic Regulations for Taught Postgraduate Degrees.

*Examination duration:* 2 hours

*Percentage of coursework, examination, etc.:* 30% CW; 70% Exam

*Grading pattern:* Standard (A+AA-…F)

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

## Part III

## Keyword Syllabus

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 assessment, different approaches
   - Information Security Management Standards

4. Legal issues
   - Computer Crimes, disk protection
   - Intellectual property
   - E-commerce law
   - Data protection issues
   - Information Security Audits

**Recommended Reading**

**Text(s)**

*Merkow & Breithaupt (2005), Information Security: Principles and Practices, Pearson*

*Greene (2006), Security Polices and Procedures: Principles and Practices, Pearson*

*Pfleeger & Pfleeger (2003), Security in Computing (3e), Prentice-Hall*

**Online Resources**