# Unit outline

| Name of unit |
| --- |
| Information Security |

| Unit description |
| --- |
| The main purpose of this unit is to enable students to master the basic theories and methods of information security so that students can understand various types of security incidents and attacks, and the technologies and methods to prevent, detect and react adversaries in the information systems. Students will learn about security architecture and models, resulting in efficiency to handle a variety of issues related to information and cyber security in any organization. Students will conduct a group presentation of their selected project related to information security. |

## SECTION 1 – GENERAL INFORMATION

### 1.1 Administrative details

| Associated higher education awards (for example, Bachelor, Diploma) | Duration (for example, one semester, full year) | Level (for example, introductory, intermediate, advanced level, 1st year, 2nd year, 3rd year) | Unit coordinator |
| --- | --- | --- | --- |
| Bachelor of ICT | One semester | 1st year, 2nd semester | |

### 1.2 Core or elective unit

Indicate if the unit is a:

☒ core unit

☐ elective unit

☐ other (please specify below):

## 1.3 Unit weighting

Using the table below, indicate the credit point weighting of this unit and the credit point total for the course of study (for example, 10 credit points for the unit and 320 credit points for the course of study).

| Unit credit points<br>Example: 10 credit points | Total course credit points<br>Example: 320 credit points |
|---|---|
| 12.5 | 300 |

## 1.4 Student workload

Using the table below, indicate the expected student workload per week for this unit.

| No. timetabled hours per week (1) | No. personal study hours per week (2) | Total workload hours per week (3) |
|---|---|---|
| 4 | 6 | 10 |

*(1) Total time spent per week at lectures, tutorials, clinical and other placements, etc.*
*(2) Total time students are expected to spend per week in studying, completing assignments, etc.*
*(3) Sum of (1) and (2) equals workload hours.*

For those students requiring additional English language support, how many additional hours per week is it expected that they will undertake?

Additional English language support: ____ hours per week

## 1.5 Delivery mode

Tick all applicable delivery modes for the unit and provide details in the following text box: If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

- ☒ Face to face on site
- ☐ E-learning (online)
- ☐ Intensive/block mode (where the unit or a face to face component is delivered in a block)
- ☐ Mixed/blended
- ☐ Distance/independent learning (untimetabled)
- ☒ Full-time
- ☒ Part-time

☐ External

☐ Fast track

☐ Other (please specify)

## 1.6 Work-integrated learning activity

If the unit includes a work-integrated learning component (where completion of the unit requires students to undertake learning in a workplace outside of their higher education provider), provide details including the rationale, the specification and methods for assessing the learning outcomes, monitoring arrangements and whether the work integrated learning is required for professional accreditation. If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

Also if available, upload copies or templates of the formal agreements with third parties for the work-integrated learning activity, using the 'Attach evidence here' function of the online form.

Refer to the TEQSA Guidance Note on Work-Integrated Learning as required (available on the TEQSA website).

N/A

## 1.7 Prerequisites and co-requisites

Are students required to have undertaken a prerequisite or co-requisite unit for this unit?

☐ Yes ☒ No

**If YES**, provide details of the prerequisite or co-requisite requirements below.

## 1.8 Other resource requirements

Do students require access to specialist facilities and/or equipment for this unit (for example, special computer access, physical education equipment)?

☒ Yes ☐ No

**If YES**, provide details of specialist facilities and/or equipment below.

## SECTION 2 – ACADEMIC DETAILS

| **Learning outcomes for the unit**<br>**On successful completion of this unit students will be able to:** |
|---|
| 1. Thoroughly understand the basic concepts of information security, information system security, and network information security, integrate theory with practice, and understand the significance of information security technology in the modern network environment<br>● Predicted difficulties: The relationship between information, information technology and information security<br>● Suggested teaching methods: Lecture, tutorial<br>● Assessment strategies: Mid-term test, final exam |
| 2. Understand the main theories of authentication, cryptography, the connotation and characteristics of symmetric key systems and public key systems, especially the common algorithms for implementing key systems<br>● Predicted difficulties: Encryption system, encryption algorithm<br>● Suggested teaching methods: Lecture, tutorial<br>● Assessment strategies: Mid-term test, final exam |
| 3. Show understanding of common information security technologies such as message authentication, digital signature, identity authentication and access control;<br>● Predicted difficulties: Certification technology<br>● Suggested teaching methods: Lecture, tutorial<br>● Assessment strategies: Mid-term test, final exam |
| 4. Meet the requirements of network environment for information security, such as firewall technology, computer virus prevention technology, network hacker attack and defense technology;<br>● Predicted difficulties: Firewall architecture<br>● Suggested teaching methods: Lecture, tutorial<br>● Assessment strategies: Mid-term test, final exam |
| 5. Understand the specifics of information security management<br>● Predicted difficulties: Information Security Architecture<br>● Suggested teaching methods: Lecture, tutorial<br>● Assessment strategies: Mid-term test, final exam |

6. To enable students to further master the scientific method of applying technology to solve practical problems according to specific conditions

- Predicted difficulties:
- Suggested teaching methods: Lecture, tutorial
- Assessment strategies: Mid-term test, final exam

| Topics included in the unit |
|---|
| 1. Information and information security risks |
| 2. Adversarial Behavior Analysis |
| 3. Information Security Architecture |
| 4. Encryption and authentication technology |
| 5. Content security technology |
| 6. Data backup and recovery technology |
| 7. System vulnerability analysis technology |
| 8. Information data protection technology |
| 9. Intrusion detection and prevention technology |
| 10. System access control and audit technology |
| 11. Computer virus prevention technology |
| 12. Future development of information security |

| Assessment tasks | | | |
|---|---|---|---|
| **Type** | **When assessed – year, session and week (for example, year 1, semester 1, week 1)** | **Weighting (% of total marks for unit)** | **Cross reference to learning outcomes** |
| Lab Participation (Individual) - Students will participate in weekly lab activities | Weekly (week 2- 11) | 20 | 1，2，4 |

| | | | |
|---|---|---|---|
| and submit their work as required.` | | | |
| Minor Assignment (Individual) - Students are expected to write Java test programs based on the contents from week 1-6. | 9 | 15 | 5 |
| Major Assignment (Group) - In groups of 2 to 3, students will write a no less than 2000 words report to discuss the information security issues and resolutions, techniques and their advantages and weakness in different practices. | 11 | 20 | 7 |
| Final Exam (Individual) - A 3-hour written exam covering key contents from weeks 1 to 12. | Exam Period | 50 | 1, 3 |

## 2.1 Prescribed and recommended reading

Provide below, in formal reference format, a list of the prescribed and recommended reading for the unit.

**Recommended Text:**

Michael E. Whitman, Herbert J. Mattord, (2017) *Principles of Information Security* 6th Edition.

**Recommended Reading:**

Jason Andress (2014) *The Basics of Information Security 2nd Edition*, Syngress