

Unit of Study: ICT5350 Securing IT Systems

Overview

In this unit students are introduced to a broad range of IT security related topics covering implementation, monitor and administration of IT infrastructure in accordance with information security policies and procedures that ensure data integrity and confidentiality. Students will apply a broad set of concepts to protect computing infrastructure from cyber security threats and attacks through a series of workshops and simulations.

Course(s)	Master of Information Technology
Credit Points	8 credit points
Duration	12 weeks (10 teaching weeks; 1 revision week; 1 final assessment week)
Level	Postgraduate Advanced
Student Workload	Students should expect to spend approximately 13 hours per week over 12 weeks (totalling approximately 156 hours) on learning activities for this unit.
Mode(s) of Delivery	On campus, Blended
Pre-Requisites	ICT5250 Computer Networks and Security
Unit Coordinator	As per current timetable
Contact Information	Consultation: 1 hour scheduled session

Unit Learning Outcomes

On successful completion of this unit, students will be able to:

- ULO1 Apply technical concepts and frameworks related to cyber security.
- ULO2 Justify strategies and measures to safeguards IT systems to mitigating risk and controls losses associated with adverse events.
- ULO3 Evaluate security risks, threats and vulnerabilities and discuss appropriate information security protection mechanisms.
- ULO4 Diagnose the cause of security incidents.
- ULO5 Develop a security incident response plans.

Weekly Schedule

Detailed information for each week's activities can be found on Unit's Weekly Modules in Canvas.

Week	Topic
Week 1	Introduction to IT security
Week 2	Access Controls part 1
Week 3	Access Controls part 2
Week 4	Security Operations and Administration
Week 5	Risk Identification, Monitoring and Analysis
Week 6	Incident Response and Recovery
Week 7	Cryptography
Week 8	Network and Communications Security part 1
Week 9	Network and Communications Security part 2
Week 10	Systems and Application Security
Week 11	Revision
Week 12	Final Assessments

Assessments

1. All assessments are compulsory.
2. To pass the unit students must:
 - achieve a total of 50% or more of marks offered; and
 - pass all individual invigilated assessments; and
 - have attempted all assessments.

Where one or more of these requirements are not met, the Board of Examiners will consider a student's overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision.







3. The Board of Examiners may grant a supplementary assessment where a student:
 - achieves a total of 45% or more; and
 - has passed all individual invigilated assessments in the unit; and
 - has attempted all assessments; and

- has a recommendation for supplementary assessment by the Unit Coordinator and the Head of Discipline.

Where one or more of these requirements are not met, the Board of Examiners will consider a student’s overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision. Attendance and engagement in class will be considered.

4. APIC awards common result grades as set out in the [Award of Grade Policy](#).
5. Detailed information for each assessment can be found on the Unit’s Home Page and in the Assessment Brief.

Detailed information for each assessment can be found on the Unit’s Home Page and in the Assessment Brief.

Assessment Task	Type	Weighting	Due	Length	ULOs
Assessment 1: Laboratory Practicum	Individual  Invigilated 	20%	Week 2, 3, 5, 7, 8	(equiv. 2000 words)	ULO1 ULO2 ULO3
Assessment 2: In-class Quizzes Quiz of key content areas to identify further support needs.	Individual  Invigilated 	20%	Week 6, 9	each 15 minutes (equiv. 2000 words)	ULO1 ULO2 ULO3
Assessment 3: Case Study: Part 1 Cause Analysis & Stakeholder Impact Analysis	Individual 	20%	Week 5	1000 words	ULO1 ULO3 ULO4
Assessment 4: Case Study: Part 2 Final security incident response plan with firewall Log Analysis, Incident report and remediation plan including constraint analysis of projected actions.	Individual 	40%	Week 12	4500 words	ULO2 ULO4 ULO5

equiv. – equivalent word count based on the Assessment Load Equivalence Guide.

Course Reserve

Course Reserve includes all required resources and reading material for the unit of study. You can access Course Reserve via [APIC Library](#) or via the Course Reserve link on the unit’s homepage.

Prescribed text(s):

Wills, M., 2019, The Official (ISC)2 SSCP CBK Reference: Amazon.com.au: Books.

Recommended Readings:

Chapple, M. and Seidl, D., 2021. Cyberwarfare: Information operations in a connected world. Jones & Bartlett Learning.

Charles P, P. and Shari Lawrence, P., 2015. Security in Computing FIFTH EDITION.

Stallings, W., 2011. Cryptography and network security: principles and practice.

Academic integrity

Ethical conduct and academic integrity and honesty are fundamental to the mission of APIC and academic misconduct will not be tolerated by the College. It is the responsibility of every student to make sure that they understand what constitutes academic misconduct and to refrain from engaging in it. Please refer to APIC's [Academic Integrity Policy](#) for further details.

Other Important Information and Links

<p>Special consideration</p> <p>If your academic work is impacted by significant documented illness, hardship, or other adverse circumstances beyond your control, you may make an application for Special Consideration. Please refer to the Assessment Policy for further details.</p>	<p>Late submission</p> <p>Penalties apply when work is submitted after the due date without approval. Please refer to the Assessment Policy for information about late submission.</p>
<p>Assessment appeals</p> <p>If you are concerned about a mark you have received for an assessment or final grade, you may apply to formally appeal the grade. Please see the Assessment Policy for further details.</p>	<p>Award of grades</p> <p>APIC awards common result grades, set out in the Award of Grade Policy.</p>
<p>Expectations of student conduct</p> <p>Students are expected to conduct themselves in a manner that is consistent with a safe and respectful study environment. More information can be found in the Student Code of Conduct.</p>	<p>Study resources</p> <p>APIC Library and Student Learning Support resources and services can be accessed via the Student Lounge or your Dashboard on the OLS (Canvas).</p>
<p>Student Services</p> <p>The Student Services team provides administrative support for students and handles enquiries about enrolment, timetables, important dates and submitting forms. More information can be found on the Student Services page on the OLS (Canvas).</p>	<p>Key dates</p> <p>Key dates through the academic year, including teaching periods, census, payment deadlines and exams can be found on the Academic Calendar section of the APIC website.</p>

Changes and Updates to the Unit of Study Guide

This Unit of Study Guide may be updated and amended from time to time. Students will be notified of any changes to the unit via the Online Learning System (Canvas) space for the unit.

This Unit of study Guide was last modified on 13th May 2024.