Module: Security 251

Module name:	Security 251
Code:	SEC251
NQF level:	6
Type:	Core – Diploma in Information Technology (all stream)
Contact time:	34 hours
Structured time:	6 hours
Self-directed time:	40 hours
Notional hours:	80 hours
Credits:	8
Prerequisites:	None

Purpose

This course covers fundamental issues and first principles of security and information assurance. The course will look at the security policies, models and mechanisms related to confidentiality, integrity, authentication, identification, and availability issues related to information and information systems. Other topics covered include basics of cryptography and network security (e.g., intrusion detection and prevention), risk management, security assurance and secure design principles, as well as e-commerce security. Issues such as organizational security policy, legal and ethical issues in security, standards and methodologies for security evaluation are also mastered.

Outcomes

Upon successful completion of this module, the student will be able to:

- Demonstrate detailed knowledge of computer and mobile security including an understanding of and the ability to apply the key terms, concepts, facts, principles, rules and theories of computer security.
- Evaluate, select and apply appropriate methods, procedures or techniques within a computer security and mobile security environment to secure a personal computer or mobile device.
- Identify, analyse and solve problems in the computer security and mobile security environment, gathering evidence and applying solutions based on evidence and procedures appropriate to computer security and mobile security.
- Have an understanding of the ethical implications of decisions and actions within a computer/mobile security environment based on an awareness of the complexity of ethical dilemmas as they pertain to the security context.
- Evaluate different sources of information, to select information appropriate to the task, and to apply well-developed processes of analysis, synthesis and evaluation within the computer/ mobile security environment.

Assessment

- Continuous evaluation of theoretical work through written assignments, a formative, and a summative test.
- Continuous evaluation of project work.
- Final assessment through a written examination.

Teaching and Learning

Learning materials

Prescribed Book

- Computer Security (2016) IT without frontiers series.

Additional material

- E-library: *Security+ Guide to Network Security Fundamentals*, 3rd Ed.pdf, O'Reilly - Malicious Mobile Code Virus Protection for Windows.chm
- Campagna, R. (2011). *Mobile Device Security for Dummies.* Wiley. ISBN: 9781118093801029

Learning activities

The teaching and learning activities consist of an amalgamation of pedagogical methodologies including formal lectures on theoretical concepts, lab exercises, and discussions. One compulsory assignment and a project must be completed during this course. The progress made on these assignments and project will guide the class discussion.

Notional learning hours

Activity	**Units**	**Contact Time**	**Structured Time**	**Self-Directed Time**
Lecture		27.0		13.0
Formative feedback		3.0		
Project	1	4.0		9.0
Assignment	1			3.0
Test	2		4.0	8.0
Exam	1		2.0	7.0
		34.0	**6.0**	**40.0**

Syllabus

- Security concepts overview.
- Type of access control methods.
- Types of authentication methods.
- Cryptography overview.
- Types of attacks.
- Remote access.
- Firewalls.
- Organizational security.
- Internet Privacy and Risk.
- Mobile problems and opportunities.
- Mobile devices and infrastructure.
- Mobile device security models.
- Legal aspects of mobile.
- Policy considerations and development.

- Mobile device management system architecture.