Module: Security 261

Module name:	Security 261
Code:	SEC261
NQF level:	6
Type:	Fundamental – Diploma in Information Technology (Infrastructure stream)
Contact time:	48 hours
Structured time:	8 hours
Self-directed time:	24 hours
Notional hours:	80 hours
Credits:	8
Prerequisites:	NWD161; ILE261

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.
- Demonstrate the ability to evaluate, select, and apply method to protect servers and clients.

Assessment

Assessment is performed using a variety of instruments:

- Continuous evaluation of theoretical work through written assignments, formative tests, and a summative test.
- Continuous evaluation through tracking of progress, offering support, guidance and provision of constant stream of opportunities to prove mastery of subject material and pursuing more challenging work as they master the basics.
- Final assessment through an examination.

Teaching and Learning

Learning materials

Prescribed books (EBSCO)

- 🕮 ***Gibson, D., 2017. CompTIA Security+: Get Certified Get Ahead: SY0-501 Study Guide (p. 560). YCDA, LLC.***

Additional material

- 🕮 ***Microsoft Security Fundamentals Exam 98-367.***

Learning activities

Learning will be facilitated by the lecturer with student centred activities that involve problem-based learning where pupils are presented with challenges that replicate the situation in the real-world environment. This will be achieved through a combination between presentation of theoretical concepts, guided exercises, group work and discussions during the module.

Notional learning hours

Contact	Distance	Other	Type of learning activities	% Learning
y	y	n	Lectures (face-to-face, limited interaction or technologically mediated)	40%
y	y	n	Tutorials: individual groups	20%
n	y	n	Syndicate groups	10%
n	y	n	Independent self-study of standard texts and references (study guides, books, journal articles)	10%
n	y	n	Independent self-study of specially prepared materials (case studies, multi-media, etc.	20%

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.
- Protecting the server and the client.