Unit Outline (Higher Education)

Institute / School:	Institute of Innovation, Science & Sustainability
Unit Title:	Networking and Security
Unit ID:	GPSIT1102
Credit Points:	15.00
Prerequisite(s):	Nil
Co-requisite(s):	Nil
Exclusion(s):	Nil
ASCED:	020113

Description of the Unit:

This course will introduce the fundamentals of networking through analysis of the Open System Interconnection (OSI) and Internet networking models. Students will learn the role of each model layer and the technologies used to provide end-to-end connectivity between computer systems and the associated networking protocols. The course will also introduce cloud computing and investigate the role of cybersecurity in securing information systems. The role of personnel and encryption to secure Internet communications will also be studied. This course will incorporate additional learning hours to support the development of students' academic and study skills.

Grade Scheme: Graded (HD, D, C, P, MF, F, XF)

Work Experience:

No work experience

Placement Component: No

Supplementary Assessment: Yes

Where supplementary assessment is available a student must have failed overall in the Unit but gained a final mark of 45 per cent or above, has completed all major assessment tasks (including all sub-components where a task has multiple parts) as specified in the Unit Description and is not eligible for any other form of supplementary assessment

Course Level:

Level of Unit in Course	AQF Level of Course					
	5	6	7	8	9	10
Introductory	✔	□	□	□	□	□
Intermediate	□	□	□	□	□	□
Advanced	□	□	□	□	□	□

Learning Outcomes:

After successfully completing this course, students should be able to:

Knowledge:

K1. Identify and explain the role and function of network connectivity in current computing.

K2. Describe and explain the principles of communication in networks and the fundamental aspects of cloud computing.

K3. Describe the role and functionality of hardware and software entities that contribute to network communications.

K4. Explain the protocols and interactions that implement network communications.

K5. Explain the critical role of cyber security in securing communication systems in terms of impacts or threats to society and individuals as well as ethical and legal considerations.

Skills:

S1. Use a variety of network services and tools to configure network settings on various network devices and operating systems.

S2. Interpret security needs of information systems in various organisational contexts..

S3. Examine and configure network settings on various network devices and operating systems.

S4. Develop the appropriate English language and academic skills to successfully study at an undergraduate level

Application of knowledge and skills:

A1. Analyse the networking architecture needs of a business or an organisation.

A2. Apply knowledge of security policies to reduce security threats.

A3. Plan and implement operational assurance programs from a security perspective.

A4. Analyse cryptographic techniques for data security.

Unit Content:

Topics may include:

- Introduction to data communications networks, network models and protocol architecture.

- IP addresses, subnet masks and the number systems used to describe them.

- Fundamentals of architectures at the application layer, common Internet based applications.

- Transmission media and their characteristics, guided and wireless media, media selection, digital and analog transmission of digital and analog data.

- Functions of data link layer, media access control, data link layer addressing, flow and error control mechanisms, data link protocols.
- Network layer protocols: Internet Protocol (IP), assigning IP addresses, address resolution, routing protocols, multicasting.
- Transport layer protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) transport layer functions, reliable and unreliable services, ports, linking to the application layer, segmentation, session management.
- Introduction to Local Area Networks (LAN), LAN components, Ethernet and Token Ring, LAN design consideration, Wireless LAN, Wide Area Networks (WAN).
- Cloud computing fundamentals, Cloud security models and the advantages and disadvantages of cloud computing.
- Security requirments, including confidentiality, integrity and availability.
- Security threats to Enterprise Networks.
- Common security countermeasures.
- Cryptography and other network security technologies.
- Planning and Implementing a Corporate Security Policy.
- Using operating system and Industry standard networking and security tools including Virtualization tools and protocol analysers.
- IT and related industry activity and research developments in the local community, and around the globe; ACS’s CBOK, SFIA and their relationship with industry; Career pathways.

Learning Task and Assessment:

Learning Outcomes Assessed	Assessment Tasks	Assessment Type	Weighting
K1, K2, K3, K4, K5, S1, S2, S3, S4, A1, A2, A3, A4.	Students will utilise their knowledge of networking protocols and security techniques to answer conceptual questions and apply their understanding to practical networking and security problems..	Assignments/laboratory tasks/oral presentations	50%-60%

Learning Outcomes Assessed	Assessment Tasks	Assessment Type	Weighting
K1, K2, K3, K4, K5, S1, S2, S3, S4, A2	Practical problems designed to test their understanding of networking concepts and protocols in the lab.	Practical lab work	10%-20%
K1, K2, K3, K4, K5, S4, A1, A2, A4	Students will provide theoretical answers and work out solutions to a range of networking and security questions.	Examinations/Tests	20% - 30%

Adopted Reference Style:

APA

Refer to the library website for more information

Fed Cite - referencing tool