Unit 2 Applied Computing – 2024

Outcome 2 Network security – Template for developing an assessment task – Plan

Outcome 2

On completion of this unit the student should be able to respond to a teacher-provided case study to examine the capabilities and vulnerabilities of a network, design a network solution, discuss the threats to data and information, and propose strategies to protect the security of data and information.

Assessment task development – Planning for the case study

Create a scenario that is a real-world example that has a level of complexity. The case study could be a small organisation that has some vulnerabilities with their existing network and faces threats to their data and information. The network must not involve manual processes and be based on an existing information system. The design of a network solution could be based on a proposed solution. Key content within the case study should be based on the targeted key knowledge and key skills. The structured questions should enable the key skills to be met.

Key knowledge	Key skills	
• applications and capabilities of LANs, Wide Area Networks (WANs) and Wireless Personal Area Networks (WPANs) • functions and characteristics of key hardware and software components of networks required for communicating and storing data and information • strengths and limitations of wired, wireless and mobile communications technology, measured in terms of cost, data storage options, data transfer rate, reliability and security • technical underpinnings of intranets, the internet and virtual private networks • risks and benefits of using networks in a global environment	• identify and describe the applications and capabilities of different networks	Content to be included in the case study should introduce students to the background of the organisation. This could include the setting of the organisation and what they do. Details should be included relating to the type of network they are using, hardware and software components and communications technology. Issues should be included within the case study for students to pick up on and write about in the structured questions.
• technical underpinnings of malware that can intentionally threaten the security of networks, such as denial of service attacks on websites, spyware, viruses and worms	• examine the impact of common network vulnerabilities	Content should be included in the case study to enable students to examine the impact of common network vulnerabilities such as denial of service attacks on websites, spyware, viruses and worms.
• design tools for representing the appearance of networks	• design a network solution with wireless capability	Students are to design a network solution with wireless capability to address the issues identified in the case study. The designs could be hand-drawn or using a software tool.
• security threats to data and information, such as improper credential management, malicious software, outdated versions of software and weak passwords	• identify and evaluate threats to the security of data and information	Content should be included in the case study to enable students to identify and evaluate the threats to the security of the organisation's data and information such as improper credential management, malicious software, outdated versions of software and weak passwords. There should be a reference to these threats and how they impact the organisation.
• data and network protection strategies, such as authentication techniques and symmetric and asymmetric encryption methods • preventative practices to reduce risks to networks, such as application of firmware, disaster recovery plans, operating system updates, software malware updates and staff procedures • technical underpinnings of intrusion detection systems (IDS) and intrusion prevention systems (IPS) • the role of ethical hacking	• propose and justify strategies to protect the security of data and information within a network	The content above should enable students to propose and justify strategies to protect the security of data and information within the organisation's network. Strategies and practices can be found in the key knowledge.
• key legislation that affects how organisations control the storage and communication of data and information: the *Health Records Act 2001*, the *Privacy Act 1988* and the *Privacy and Data Protection Act 2014* • ethical issues arising from data and information security practices	• identify and discuss possible legal and ethical issues arising from ineffective data and information security practices	Content should be included in the case study for students to be able to clearly identify the relevant legislation impacting the organisation. This could be the Health Records Act 2001, Privacy Act 1988 or the Privacy and Data Protection Act 2014. Details describing how the organisation controls the storage and communication of data and information should be included. Students should be able to clearly identify some legal and ethical issues arising from the organisation's ineffective data and information security practices.