<table>
<tr><th colspan="3">Unit 2 Applied Computing – 2024
Outcome 2 Network security – Template for developing an assessment task – Blank</th></tr>
<tr><td colspan="2"><b>Outcome 2</b>
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.</td><td rowspan="8"><b>Assessment task development</b></td></tr>
<tr><td><b>Key knowledge</b></td><td><b>Key skills</b></td></tr>
<tr><td>• 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</td><td>• identify and describe the applications and capabilities of different networks</td></tr>
<tr><td>• technical underpinnings of malware that can intentionally threaten the security of networks, such as denial of service attacks on websites, spyware, viruses and worms</td><td>• examine the impact of common network vulnerabilities</td></tr>
<tr><td>• design tools for representing the appearance of networks</td><td>• design a network solution with wireless capability</td></tr>
<tr><td>• security threats to data and information, such as improper credential management, malicious software, outdated versions of software and weak passwords</td><td>• identify and evaluate threats to the security of data and information</td></tr>
<tr><td>• 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</td><td>• propose and justify strategies to protect the security of data and information within a network</td></tr>
<tr><td>• key legislation that affects how organisations control the storage and communication of data and information: the <i>Health Records Act 2001</i>, the <i>Privacy Act 1988</i> and the <i>Privacy and Data Protection Act 2014</i>
• ethical issues arising from data and information security practices</td><td>• identify and discuss possible legal and ethical issues arising from ineffective data and information security practices</td></tr>
</table>

© VCAA