VCE Applied Computing 2025–2028

Video 5

Background to Unit 2 Outcome 2
Applied Computing

VICTORIAN CURRICULUM AND ASSESSMENT AUTHORITY
VICTORIA State Government

Acknowledgement of Country

The VCAA respectfully acknowledges the Traditional Owners of Country throughout Victoria and pays respect to the ongoing living cultures of First Peoples.

VCE Applied Computing 2025–2028

Video 5

Background to Unit 2 Outcome 2
Applied Computing

VICTORIAN CURRICULUM AND ASSESSMENT AUTHORITY
VICTORIA State Government

Purpose of this presentation

- Overview of Unit 2 Outcome 2 Applied Computing
- Major changes to Unit 2 Outcome 2
- Outcome statement
- Key knowledge
- Key skills
- Assessment tasks

Unit 2 Outcome 2

Changes to Unit 2 Outcome 2

- Cyber security incident
- Emerging trends/AI
- Cryptography
- Frameworks
- Updated assessment tasks

Unit 2 Outcome 2

From the outcome statement

- Respond to a teacher-provided case study to examine a cyber security incident or a network vulnerability, evaluate the threats to a network, and propose strategies to protect the security of data and information on the network.

Unit 2 Outcome 2 – Key knowledge

- emerging trends in cyber security, such as:
  - security measures (multi-factor authentication)
  - regulatory compliance
  - artificial intelligence-based (AI) threat detection
  - Zero Trust Architecture
  - use of cryptography for protection strategies

Unit 2 Outcome 2 – Key knowledge

- functions and characteristics of key hardware and software components of networks required for communicating and storing data and information, such as:
  - routers for connecting multiple networks
  - switches for connecting multiple devices in a network
  - firewalls for monitoring and controlling incoming and outgoing network traffic
  - data storage and backup systems
  - network security software (firewall software, antivirus software, Darktrace AI) for protecting networks from threats and vulnerabilities
  - technical underpinnings of intrusion detection systems (IDS) and intrusion prevention systems (IPS)

Unit 2 Outcome 2 – Key knowledge

- strengths and limitations of wired, wireless and mobile communications technology, measured in terms of:
  - cost
  - data storage options
  - reliability
  - security
- technical underpinnings of intranets, the internet and virtual private networks
- applications and capabilities of Local Area Networks (LANs), Wide Area Networks (WANs) and Wireless Personal Area Networks (WPANs)

Unit 2 Outcome 2 – Key knowledge

- risks of using networks in a global environment, such as:
  - cyber security threats
  - data privacy
  - legal compliance
  - unauthorised network access
- technical underpinnings of malware that can intentionally threaten the security of networks, such as:
  - spyware
  - viruses
  - worms
  - ransomware

Unit 2 Outcome 2 – Key knowledge

- security threats to data and information on networks, such as:
  - denial of service attacks
  - improper credential management
  - malicious software
  - outdated versions of software
  - weak passwords

Unit 2 Outcome 2 – Key knowledge

- practices for reducing risks and mitigating threats to networks, such as:
  - application of firmware
  - multifactor authentication
  - backup strategies
  - operating system updates
  - software malware updates
  - staff procedures

Unit 2 Outcome 2 – Key knowledge

- cryptographic techniques to protect data and networks, such as:
  - ciphers (Caesar cipher, Vigenère cipher, polyalphabetic cipher)
  - symmetric encryption (AES)
  - asymmetric encryption (ECDH, ECDSA, RSA)
- emergence of artificial intelligence in providing network security mechanisms, such as:
  - machine learning algorithms that analyse network traffic patterns
  - provision of real-time monitoring and notification

Unit 2 Outcome 2 – Key knowledge

- the role of ethical hacking, such as identifying vulnerabilities and weaknesses in networks
- key legislation and industry frameworks that affect how organisations ethically control the security and communication of data and information:
  - Essential Eight
  - *Health Records Act 2001* (HPP 2, 4, 5)
  - Information Security Manual (ISM) (Guidelines for Networking: Encryption; Segmentation and segregation; Network access controls; Confidentiality and integrity of wireless network traffic; Wireless network footprint)
  - *Privacy Act 1988* (Cwlth) (APP 1, 6, 11)
  - *Privacy and Data Protection Act 2014* (IPP 2, 4, 5).

Unit 2 Outcome 2 – Key skills

- identify and examine a cyber security incident or a network vulnerability
- identify and describe the key components of networks
- describe the capabilities of different networks
- identify and evaluate the impact of network vulnerabilities and threats to the security of data and information
- identify and discuss possible legal and ethical issues arising from ineffective security strategies
- propose and justify strategies to protect the security of data and information within a network.

Unit 2 Outcome 2 – Assessment task

Suitable tasks for assessment in this unit may be selected from the following:

- A teacher-provided case study with structured questions that investigates a cyber security incident and how it could be prevented in the future.
- A teacher-provided case study with structured questions that investigates a network, its vulnerabilities and how these could be mitigated.

Contact

- Phil Feain – Digital Technologies Curriculum Manager (VCAA)
- Ph: (03) 9059 5146
- Philip.Feain@education.vic.gov.au

Authorised and published by the
Victorian Curriculum and Assessment Authority