



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

COURSE	:	COMPUTER SECURITY
COURSE CODE	:	CSC662
EXAMINATION	:	OCTOBER 2026 (MOCK)
TIME	:	3 HOURS

MARKING SCHEME NOTES

1. This marking scheme accompanies the CSC662 mock paper (October 2026).
Computed answers show working; theory answers are supported by lecture slides (not lecturer-marked); verbatim quotes are omitted in this public build; slide citations are retained.
2. Supported theory marking points quote the lecture decks; any unresolved slot would remain a visible placeholder.
3. Part A = $10 \times (2 + 6)$; Part B = $2 \times (5 + 5)$; total = 100 marks.
4. Computed: 1 slot(s). Supported theory: 23 slots. Placeholders: 0.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of 15 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

Labels: computed / supported by lecture slides (not lecturer-marked) / placeholder. No official marking scheme exists for the real CSC662 papers; this is generated for the mock.

Entailment labels: supported = the private quote directly supports the point (or the point passed the stem-overlap gate); partly supported = partial/ambiguous support; not supported = no support. Quote text is omitted here; verdicts come from private verification.

Part A: 10 x (2 + 6) = 80 marks. Part B: 2 x (5 + 5) = 20 marks. Total: 100 marks. Slots: 1 computed, 23 supported by lecture slides, 0 placeholder.

Methods: computed answers use verified solvers. Theory answers are supported by lecture slides (not lecturer-marked). Each point carries a deck/slide citation and overlap score; verbatim quote text is omitted from this public build. Low overlap is flagged for human review.

PART A - QUESTION 1

A1a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

List two types of malware described in the course and, for each, state one characteristic behaviour that distinguishes it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans masquerade as helpful or harmless programs while carrying out malicious actions such as stealing data or opening the system to further malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.53
2	Worms exploit a vulnerability in the computer system in order to cause harm.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.88

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 051 - Software Security, slide 12

A1b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

State six techniques or behaviours by which malware attacks and propagates through computer systems, as described in the course, covering executable infection methods, historical propagation examples, and how specific malware types operate on infected hosts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can infect an executable by appending its virus body to the program and saving the program's entry point inside the virus body.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.64
2	A virus can replace the program's entry point with a jump to the virus body, which later restores the original entry point and jumps to it after executing.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.61
3	In EXE infection, the virus overwrites the program header to switch the entry point to the virus and jumps to the original entry point during execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	partly supported	0.46 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The Morris worm used a debugging feature of sendmail for remote execution and propagated across the Arpanet, penetrating about 6,000 computers.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.31 LOW
5	Rootkits mask malicious processes and software in infected systems to ensure privileged remote access, and are usually installed after a vulnerability has been found.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.65
6	Spyware spies on users by stealing logins and passwords, documenting sites visited, logging keystrokes, and redirecting browsers to unwanted sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.86

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART A - QUESTION 2

A2a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how a substitution cipher conceals the original message, and state what serves as the key in such a cipher.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The plaintext letters are swapped for other letters, and the transformed text produced is the ciphertext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	partly supported	0.38 LOW
2	The rule governing the letter replacement acts as the key of the cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.17 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 031 - Classical Cryptography, slide 4

A2b - 6 marks - computed - matches lecture slide 15 (standard tableau)

Question:

*Decrypt the following ciphertext using the Vigenere cipher with the key CIPHER. Use the standard 26 x 26 Vigenere tableau, writing the key over the message and repeating it as necessary.
UMRBVVNWVPREQE*

Answer: SECURELOGINNOW

The 26 x 26 Vigenere tableau is printed in the question paper.

Working:

Standard 26 x 26 tableau, A=0; key repeated over the ciphertext.
Ciphertext: UMRBVVNWVPREQE
Key: CIPHERCIPHERCI
Letter-by-letter: $C - K \bmod 26 = P$
U (20) - C (2) = 18 -> S
M (12) - I (8) = 4 -> E
R (17) - P (15) = 2 -> C
B (1) - H (7) = 20 -> U

V (21) - E (4) = 17 -> R
 V (21) - R (17) = 4 -> E
 N (13) - C (2) = 11 -> L
 W (22) - I (8) = 14 -> O
 V (21) - P (15) = 6 -> G
 P (15) - H (7) = 8 -> I
 R (17) - E (4) = 13 -> N
 E (4) - R (17) = 13 -> N
 Q (16) - C (2) = 14 -> O
 E (4) - I (8) = 22 -> W
 Plaintext: SECURELOGINNOW

Suggested marks: 1 mark for the key/table setup; 4 marks for the letter-by-letter working; 1 mark for the complete answer.

Confidence: computed - matches lecture slide 15 (standard tableau).

PART A - QUESTION 3

A3a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State the two stages of the biometric authentication process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage, which involves acquisition, creation of master characteristics and storage of master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.86
2	The authentication stage, which involves acquisition(s), comparison and decision.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.83

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 5

A3b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Discuss six aspects of biometric mechanisms and technologies used for user authentication, covering how biometrics are defined, how they are categorised, and the characteristics of specific biometric technologies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A biometric is defined as a physiological or behavioural characteristic of a human being that can distinguish one person from another and can theoretically be used for identification or verification of identity.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.92
2	Biometric applications available today are categorised into two sectors, namely psychological and behavioural.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.67

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The psychological category of biometrics includes iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.70
4	The behavioural category of biometrics includes voice, typing pattern and signature.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.57
5	Retinal scanning is very efficient and cannot be spoofed, but it suffers from disadvantages such as the user having to look directly, a high failure-to-enrol ratio, and acceptability concerns about light exposure and hygiene.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 9 072 - Biometrics and Authentication::s09::1	partly supported	0.12 LOW
6	Fingerprint biometrics have disadvantages including racial issues, dirt, grime and wounds, placement of the finger, too large a database to process, and the need for liveness detection because they can be spoofed.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.13 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7; 072 - Biometrics and Authentication, slide 9

PART A - QUESTION 4

A4a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how the classes of threats described in the course can affect the confidentiality, integrity and availability of information assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure threats such as snooping, sniffing and wiretapping give unauthorised access to information, which harms confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported	0.27 LOW
2	Deception and disruption threats involve modification of data, which harms integrity.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.25 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 011 - Introduction to Computer Security, slide 10

A4b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Refer to your answer in (a). Discuss the Samy worm as a case study of script injection, covering how the malicious script is delivered and executed, how the worm spread itself, and the scale of the resulting infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile using document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
2	The worm obtained the list of the user's heroes by issuing a GET request on a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.38 LOW
3	The worm added Samy as a friend by performing XML-HTTP on the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
4	Any visitor to an infected user's page had their own profile and friends list infected, so the worm spread from profile to profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW
5	The infection eventually reached about 1,000,000 MySpace profiles, showing the scale of the impact.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.50
6	The underlying weakness is that any web application returning user input without filtering is a potential XSS vulnerability, which is what allowed the injected script to be stored and served.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.56

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 052 - Web Security, slide 13; 052 - Web Security, slide 15

PART A - QUESTION 5**A5a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

Explain the Chinese Wall model as a formal security model, stating the concern it is designed to address and how its access decisions differ from static policies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The model was proposed by Brewer and Nash to address conflicts of interest faced by consultants or contractors.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.56
2	Access rights are not fixed but depend dynamically on the subject's history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported	0.30 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 27

A5b - 6 marks - supported by lecture slides (not lecturer-marked)**Question:**

Describe six (6) points about the access control matrix, access control lists and capabilities as access control structures, covering what each structure represents and one advantage or disadvantage of each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is identified as a basic access control structure.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported (stem gate)	0.60
2	A stated advantage of the access control matrix is that it is easy to verify.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported (stem gate)	0.50
3	A stated disadvantage of the access control matrix is poor scalability.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported (stem gate)	0.50
4	An access control list is described as an object-centered description of access rights.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.83
5	A stated advantage of ACLs is easy access to object access rights.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.83
6	A stated disadvantage of ACLs is difficulty of revocation.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.50

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples n<3; widened via topic+marks (any command).

Citations: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 8

PART A - QUESTION 6

A6a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State two ways in which an intrusion detection system can support the detection and defence against attacks on a computer system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can confirm whether an attack succeeded or failed by examining host-based IDS log entries.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported	0.25 LOW
2	An IDS can monitor network traffic even when it is encrypted.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported (stem gate)	0.62

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 062 - Intrusion Detection System, slide 14

A6b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Describe six threat classes or attack techniques covered in the course and, for each, state one countermeasure or protective mechanism that can be applied against it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Threats are potential violations of security, distinct from attacks which are actual violations, so countermeasures must guard against possible rather than only realised violations.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	partly supported	0.27 LOW
2	Software threats include modification of program code, which can be countered by protecting code integrity.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.20 LOW
3	Viruses and self-replicating code form a software threat class that must be defended against.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.36 LOW
4	Buffer overflow is a software threat class, and one countermeasure against it is applying software updates/patching.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 19 011 - Introduction to Computer Security::s19::1	partly supported	0.20 LOW
5	Script injection such as XSS is a software threat class that must be mitigated in web applications.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.27 LOW
6	SQL injection is a software threat class, and one countermeasure against it is validating and sanitising user input.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.18 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 011 - Introduction to Computer Security, slide 19; 011 - Introduction to Computer Security, slide 9; 051 - Software Security, slide 2

PART A - QUESTION 7

A7a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how the chain of trust works in the Trusted Computing architecture, referring to the role of the TPM and the measurement of each stage.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the platform measures and validates the following stage, with the resulting measurements stored in the TPM's Platform Configuration Registers (PCRs).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.27 LOW
2	The chain begins at the hardware TPM and then proceeds through the software layers (RTM, TPM Software Stack, BIOS, kernel), so that the whole platform ends up verified as being in a trusted state.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.28 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 073 - Trusted Computing, slide 8

A7b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

State six components and functions of the NGSCB architecture, focusing on the Nexus and the Nexus Computing Agent (NCA).

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	NGSCB has two primary system components, namely the Nexus and the Nexus Computing Agent (NCA).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	partly supported	0.29 LOW
2	The Nexus is a special kernel that forms the core of the trusted operating environment.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.62
3	The Nexus is a security kernel that is authenticated on boot.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.80
4	The Nexus authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.75
5	The Nexus provides the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.60
6	The NCA is a trusted software component that runs in trusted mode and communicates with the Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.86

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 073 - Trusted Computing, slide 13; 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 8

A8a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

List TWO (2) password security controls that can be applied to password files and user accounts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Applying access control to password files	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.80
2	Deactivating accounts after multiple failed login attempts	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.71

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 12

A8b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how single sign-on, Kerberos and smart cards support user authentication in large distributed environments. Your answer should cover the motivation for single sign-on, the solutions available, how Kerberos handles a user login, and where these mechanisms fit among alternative authentication approaches.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on is motivated by reducing the need for users to memorize passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
2	Single sign-on also reduces the time users spend typing passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.38 LOW
3	Single sign-on lowers the effort of password maintenance.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
4	Client-server architectures such as Kerberos and Active Directory are one solution for single sign-on.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.60
5	In Kerberos login, the user enters a user name and password at a client workstation.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.71

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The hash of the user's password becomes the secret key of the client or user.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	1.00

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 19

PART A - QUESTION 9

A9a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain the difference between morals, ethics and laws as three distinct forms of guidance on conduct.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct, forming the foundation of social behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.64
2	Laws are formal rules of conduct imposed by a sovereign authority such as a government on its subjects or citizens.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	1.00

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 071 - Ethics and Computer Security, slide 5

A9b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain six ways in which a professional code of ethics and conduct, such as the ACM code, guides the behaviour of a computing professional.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code of ethics is a documented set of acceptable behaviours for a professional group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.62
2	The code is defined by the professional group itself.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.40 LOW
3	It identifies which specific actions are appropriate or inappropriate.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	1.00

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	It requires the professional to contribute to society and human well-being, treating all people as stakeholders.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.70
5	It obliges the professional to respect privacy and honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	partly supported	0.33 LOW
6	It directs the professional to give comprehensive and thorough evaluations of computer systems and their impacts, including possible risks.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.82

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12; 071 - Ethics and Computer Security, slide 6

PART A - QUESTION 10

A10a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) typical locations where IDS sensors are placed in a network-based IDS architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be positioned immediately inside the firewall.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.33 LOW
2	A sensor can be positioned on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.25 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 062 - Intrusion Detection System, slide 7

A10b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Discuss the preventive network security mechanisms that an organization can deploy to protect its network, covering firewalls, proxy servers, network segmentation, remote access VPN and intrusion detection/prevention systems. Provide six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing network traffic according to predetermined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	A proxy server improves data security and network performance by acting as a firewall and web filter, sharing connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.79
3	Network segmentation creates boundaries between segments whose computing assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.77
4	A remote access VPN gives individual hosts or clients remote and secure access to the organization network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access restricts each user to only the access and permission required to fulfill the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.64
6	IDS/IPS detect or prevent network attacks such as brute force attacks, Denial-of-Service attacks and exploits of network vulnerabilities.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.85

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 061 - Network Security, slide 3; 061 - Network Security, slide 4

PART B - QUESTION 1

B1a - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

Discuss the ethical impacts of technology by examining how professional codes of ethics, such as the ACM code, guide a computing professional's conduct, and evaluate the limitations of such codes in addressing the ethical impacts of technology.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Recognise that the ACM, founded in 1947, has a code of ethics and professional conduct that professionals can refer to when judging the ethical impact of their technological work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.50
2	Note that other professional bodies such as AITP provide education and forums that help members reason about relevant IT issues and their ethical implications.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.41 LOW
3	Acknowledge that the IEEE Computer Society is another professional body that maintains a code relevant to the ethical conduct of computing professionals.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.25 LOW
4	Explain that a professional code may not reflect the ethics of every member of the group, so it cannot fully capture the diverse ethical impacts of technology on different stakeholders.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.44 LOW
5	Discuss that such codes are often not enforceable because they are codes of conduct rather than legal documents, limiting their power to regulate the ethical impacts of technology.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.33 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 071 - Ethics and Computer Security, slide 7; 071 - Ethics and Computer Security, slide 9

B1b - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain five ethical responsibilities that the hospital's information technology unit owes to patients with respect to the privacy and accuracy of their medical records, drawing on the ethical dimensions of computer security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The unit must safeguard patients' personal information as a matter of privacy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported	0.25 LOW
2	The unit must ensure that stored patient information is accurate and can be verified as faithful.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported	0.10 LOW
3	The unit must respect who owns information about patients and control how that information is sold or exchanged.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.55
4	The unit must govern what information a person is entitled to obtain about others and how that information may be used.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.50
5	Information specialists in the unit carry definite duties to act within ethical, moral and legal limits.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.58

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 071 - Ethics and Computer Security, slide 13; 071 - Ethics and Computer Security, slide 3

PART B - QUESTION 2

B2a - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

State FIVE (5) points about software insecurity and buffer overflows, covering their root causes, how a stack buffer overflow hijacks execution, and techniques used to strengthen software security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Software insecurity arises because attackers can modify system resources that are critical for program execution, such as the instruction pointer and function call addresses.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.72

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	A key source of software insecurity is the failure to validate user input.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.86
3	Buffer overflows are among the most widely used exploitation techniques.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.71
4	Without proper bound checking, a local buffer can overflow into the adjacent upper stack area.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.92
5	By controlling the buffer content, an attacker can overwrite the return address with an arbitrary value and thereby hijack the execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.86

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples n<3; widened via topic+marks (any command).

Citations: 051 - Software Security, slide 21; 051 - Software Security, slide 30

B2b - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

Windows provides several security mechanisms for managing users, objects and access. Explain FIVE (5) points about these Windows security mechanisms, covering the directory service used to organise resources, the access rights model, the role of the registry, and why the complexity of these mechanisms can itself be a weakness.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Active Directory is an LDAP-like directory service introduced in Windows 2000 that organises system resources such as users, groups, credentials, policies and trust.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.59
2	Access rights describe what a subject can do to an object and are encoded as a 32-bit mask, with standard rights common to most object types and object-specific rights tailored to each class.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 16 041 - Windows Security::s16::1	partly supported	0.23 LOW
3	The registry is a hierarchical database holding critical system information, and certain hives such as SAM and Security store security-relevant data.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 4 041 - Windows Security::s04::1	partly supported	0.33 LOW
4	Windows contains complex mechanisms for user account and object management and access control, and discretionary access control enables fine-grained control over heterogeneous entities.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.59
5	The complexity of Windows security mechanisms is also its enemy, because misconfiguration and implementation bugs can lead to severe security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.79

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 041 - Windows Security, slide 16; 041 - Windows Security, slide 21; 041 - Windows Security, slide 4; 041 - Windows Security, slide 6

End of marking scheme.