UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2021/2022

COURSE NAME	:	INFORMATION SECURITY STANDARDS
COURSE CODE	:	BIS 33203
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2022
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. THIS FINAL EXAMINATION IS AN **ONLINE** ASSESSMENT AND CONDUCTED VIA **OPEN BOOK.**

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

SECTION A

Instruction: State whether TRUE (T) if the following scenario does not violate the policy or FALSE (F) if it violates the policy.

Based on Universiti Tun Hussein Onn Malaysia (UTHM) Computer Installation and Use Security Policy in Appendix A.

Q1 A staff orders food delivery from FoodPanda mobile application using UTHM WiFi network.

(1 mark)

Q2 A staff installs Netflix on his UTHM laptop and register using personal Google account.

(1 mark)

Q3 A staff does not use screen lock mechanisms on his personal smartphone that is connected to UTHM Google Account.

(1 mark)

Q4 Dr. Amy shares BIS students' Siswa UTHM email address to her friend for laptop promotions.

(1 mark)

Q5 A staff uses Adobe Illustrator software with UTHM license to design a brochure for "Visit Thailand 2022" program organized by Batu Pahat Tourism Agency.

(1 mark)

Q6 Human Resource department organizes a series of Cyber Safe training. All staff in the department is compulsory to participate and unreasonable absenteeism is subjected to a disciplinary action.

(1 mark)

Q7 A staff shared a viral message claiming a teenager died due to Covid-19 vaccine on Facebook using his personal smartphone that is connected to Celcom data plan during a lunch break.

(1 mark)

Q8 A staff downloads The Batman movie from BitTorrent using his own UniFi network on his personal laptop. He uploads the movie on his personal Google Drive account. He then shares the movie to his friends' UTHM Google account.

(1 mark)

Q9 IT Incident Response Unit detected Dr. Atikah's laptop contains of web scripting virus that has spread through network. The unit requests Dr. Atikah to bring her laptop for repair and maintenance. She deletes all browsing activities and uninstalls some programs from the past 14 days before sending her laptop to IT Incident Response Unit.

(1 mark)

Q10 Deputy Dean of Academic shares academic syllabus information to academic staff using UTHM Google Drive and sets an access restriction to UTHM staff only. Dr. Zack screenshots part of the syllabus information using his personal smartphone and sends it to his friend in another university through WhatsApp.

(1 mark)

SECTION B

Q11 Your team is consulting KPJ Healthcare to prepare information security policy and best practices to their Internet of Things (IoT) medical devices. The value of threats probability and impact level are 1 for Minor, 2 for Medium, and 3 for Major. **Table Q11** presents the initial assessment of the IoT devices.

Table Q11

No.	Threats to the IoT devices	Probability	Impact
1	Password attack	3	3
2	Human error	1	3
3	Malicious insider	1	3
4	Malfunction devices	2	2
5	Outdated devices	2	3

Based on the scenario, answer the following questions:

(a) Illustrate a risk evaluation map based on **Table Q11** with acceptable risk level is 1.5.

(6 marks)

(b) Propose a Statement of Applicability for unacceptable risks in **Q11(a)** by referring to Annex A ISO/IEC 27001:2005.

(10 marks)

(c) (i) Describe **ONE (1)** encryption protocol to protect data in-transit for KPJ IoT medical devices.

(4 marks)

(ii) Would you encourage KPJ Healthcare uses the same key in **Q11(c)(i)** for digital signatures?

(1 mark)

(iii) Discuss your answer in **Q11(c)(ii)** based on the National Institute Standard and Technology (NIST) Recommendation for Key Management - Part 1: General.

(5 marks)

Q12 During one of online classes, a lecturer has allegedly insulting a student for not submitting an assignment. The student, Camilla, was secretly recording the lecturer's clip. She then posted the video on her Twitter account. Subsequently, the video went viral and Camilla deleted her Twitter account. The viral video received various positive, negative and offensive comments from netizen. The university management performed an investigation and was able to detect Camilla's identity. The case had been forwarded to the police and had been investigated under Communications and Multimedia Act 1998.

Based on the scenario, answer the following questions:

(a) Discuss **ONE (1)** potential ethical dilemma for each of the ethical issues that relevant with the given scenario.

(12 marks)

(b) Justify the potential Section in the Communications and Multimedia Act 1998 that can be charged to Camilla.

(8 marks)

(c) Discuss if other students who forwarded the viral video through WhatsApp group medium can be charged in the same Section in **Q12(b)**.

(5 marks)

Q13 V-Key announced that V-OS, V-Key's core patented technology, is the world's first virtual secure element to receive a Common Criteria Evaluation Assurance Level (EAL) rating of 3+, derived from the U.S. Government's Protection Profile for General Purpose Operating Systems. V-OS is similar to a smartcard chip, also known as a hardware secure element. V-OS creates an isolated virtual environment within mobile applications to safely store cryptographic keys. This demonstrates the degree of protection that V-OS provides against the most advanced hacking techniques. Everything from V-OS App Protection to V-OS Cloud Solutions benefits from the assurance provided by V-OS' EAL3+ certification. V-Key continually invests in certifications because it is an important pillar of trust, both between V-Key and its customers, and between customers and their end-users. "We are glad that V-Key has taken great strides and again pushed the boundaries by securing the EAL3+ certification. This is testament of the maximum assurance and rigor of V-OS, providing world class mobile security," said Mr. Edwin Low, Director of Innovation & Tech Ecosystem, Infocomm Media Development Authority of Singapore.

Based on the scenario, answer the following questions:

(a) Describe the Target of Evaluation (ToE) and Sponsor.

(3 marks)

(b) Discuss **TWO (2)** differences between Level 2 and Level 3 for Common Criteria Evaluation Assurance.

(6 marks)

(c) Assume you are working for an airline agency and want to recommend the vendor for employee smart identification card at your workplace.

Justify **TWO (2)** arguments of your recommendation based on the certificate evaluation and relevant cyber security threats to smart cards.

(10 marks)

-END OF QUESTIONS –

FINAL EXAMINATION
APPENDIX A

SEMESTER / SESSION	:	SEM II 2021/2022	PROGRAMME CODE	:	BIS
COURSE NAME	:	INFORMATION SECURITY STANDARDS	COURSE CODE	:	BIS 33203

Universiti Tun Hussein Onn Malaysia (UTHM) Computer Installation and Use Security Policy

Focus : A computer installation that supports one or more business applications

Principle : Staff running the installation should be made aware of the key elements of information security and why it is needed and understand their personal information security responsibilities.

Objective : To ensure that staff running the installations apply security controls and prevent the security of information used in the computer installation from being compromised.

1. There should be an information security policy that applies to the computer installation and use. Staff employed in the computer installation and use should be aware of the policy and comply with it.
2. Staff employed in the computer installation and use should:
   a. take part in a security awareness program
   b. be provided with information security education/training, such as via computer-based training
   c. be supplied with specialized security awareness material, such as brochures, reference cards, posters, and intranet-based electronic documents.
3. Staff employed in the computer installation and use should be made aware of:
   a. the meaning of information security
   b. why information security is needed to protect the installation and use
   c. the important of complying with information security policies and applying associated standards/procedures
   d. their personal responsibilities for information security
4. Staff employed in the computer installation and use should be made aware that they are prohibited from:
   a. using any part of the installation and use without authorization or for purposes that are not work-related
   b. making sexual, racist, or other statements, which may be offensive (e.g. by using corporate Google account or the Internet)
   c. making obscene, discriminatory, or harassing statements, which may be illegal (e.g. by using corporate Google account or the Internet)
   d. downloading/storing illegal material (e.g. by using corporate Google account or the Internet)
   e. using unauthorized installation components (e.g. installing unauthorized third-party software)
   f. unauthorized copying of information or software
   g. disclosing confidential information (e.g. student records, syllabus designs)
   h. compromising passwords (e.g. by writing them down or disclosing them to others)
   i. using personally identifiable information for business purposes unless explicitly authorized
   tampering with evidence in the case of incidents that may require forensic investigation.