Muhammad Izham Bin Norhamadi
B032020039

No. Date

Question 1

a. Anti-Fake News Act 2018.

b. 1) Prevents fake news or publication that aims to cause public fear and alarm
2) Prevents false reports regarding COVID-19
3) Provides proper punishments to bad actors spreading fake news

c. 1) Raises concerns that the Act was incompatible with international human rights to freedom of expression
2) Can be used to censor speech and punish government critics
3) The Ordinance is overly vague as to as to what counts as fake news
4) Penalties for offences under the Ordinance are grossly disproportionate as possibility for compounding punishment for viral content.

d. 1) Provide a comprehensive and clear list as to what counts as fake news and their medium
2) Reform other laws that limit the right to freedom of expression, in particular by repealing the Sedition Act and reforming the Communications and Multimedia Act

STANDARD

Muhammad Izham Bin Norhamadi
B032020039

No: Date:

Question 2

a. 1) Communications and Multimedia Act 1998
2) Penal Code

b. 1) Communications and Multimedia Act is under MCMC meaning people can file report to MCMC under this act
2) Communication and Multimedia Act provides and regulates converging communications and multimedia for incidental matters
3) Section 506 protects victims from threats with promise of injury and intent to cause harm to victim.

c. 1) Harassment
- refers to persistent pattern of mean and dangerous messages sent with intent of harming

2) Cyberstalking
- severe form of cyberbullying that can go to extent of physical harm threats, false accusation, and monitoring

d. 1) Refrain from responding to it as the bully wants the victim to fight back
2) Gather evidence of bullying and seek non-governmental organizations that helps cyberbullying victims
3) Report cyberbullying to CyberSecurity Malaysia
4) Block cyberbully from posting rude comments

Question 3

a. 1) General principle
- A data user shall not process personal data about an individual unless that individual has given consent to the processing

2) Notice and choice principle
- A data user is required to give a written notice informing individual that their personal data is being processed and the purpose for data being collected

3) Disclosure principle
- Personal data shall not, without consent of data subject, be disclosed for any purpose

4) Security principle
- Data user must take practical steps to ensure the security, reliability and integrity of the personal data

b. 1) Prevention or detection of crime
2) Assessment or collection of tax or duty

c. 1) Selling personal data
2) Unlawful collection
3) Transfer data without adequate protection
4) Disclosure without consent

d. 1) Right to access
2) Right to prevent processing likely to cause damage or distress
3) Right to prevent processing for direct marketing purpose
4) Right to withdraw consent
5) Right to correct
6) Right to be informed

Question 4

a. 1) Password policy
- All users must have a unique user ID and password that confirms to the company password standard
- Users must not share their password with anyone regardless of title or position
- If a password is compromised, it must be reported immediately to help desk and a new password must be requested

2) Password standard
- Minimum of eight upper and lowercase alphanumeric characters
- Must include at least one special character (such as *, &, #, ※, !, or @)
- Must not include user's name, the company name, or location

b. 1) Overview - Background information on what issue the policy address
2) Purpose - Why the policy was created
3) Targeted audience - To whom the policy is applicable
4) Policy - A complete but concise description of the policy

c. 1) Write for your audience
2) Write short sentences
3) Limit a paragraph to one subject
4) Be concise
5) Don't use jargon or technical terms when everyday words have the same meaning

d. 1) Readers understand documents better
2) Readers prefer plain language
3) Readers locate information faster
4) Documents are easier to update
5) It is easier to train people.

Question 5

a. CC was prepared predominantly by unifying pre-existing standards (TCSEC, ITSEC, and CTCPE) to make sure companies selling computer-related products for government departments may have a standard set to be evaluated against

b. CC provides the assurance that the specification process, its implementation, and evaluation of the products related to computer security have been carried out through rigorous and standard protocols at a level corresponding to the target environment for actual use

c. 1) Evaluation is a costly process and the vendor's return on that investment is not necessarily a more secure product
2) Evaluation focuses primarily on assessing the evaluation documentation, not on the actual security
3) The effort and time necessary to prepare evaluation evidence is cumbersome
4) Industry input generally has little impact to the process as a whole

d. 1) CESG Tailored Assurance Service (CTAS) schemes for assurance of goverment systems
2) CEGS Claims Tested Mark (CCT Mark) aims at handling less exhaustive assurance requirements for products and services in a cost and time efficient manner
3) Vision Statement - Technical Communities will be focused on authoring Protection Profiles (PP) that support their goal of reasonable, comparable, reproducible and cost-effective evaluation results