1. Consider a student information system (SIS) in which students provide a university student number (SN) and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system and indicate the degree of the importance of the requirement.

* Confidentiality: students should not be able to access other students’ data like their SN and card details and the data should be kept away from other external parties
* Integrity: student details should not be altered by other parties or even students themselves in this case as the student number would be rigid
* Availability: students should be able to use their cards as needed

2. Which of the following attacks are attacks on (1) confidentiality, (2) integrity, (3) availability?

(a) Opening my neighbour’s letter without their consent - (1)

(b) Installing malware on a data server that has private information in order to transmit the data to attackers - (2)

(c) Conducting a ransomware attack that encrypts data on targeted computers so that the authorised parties cannot use it in order to compel them to pay a ransom to the attacker – (3)

(d) Deliberately disrupting a server room’s power supply in order to take those servers offline – (3)

(e) An employee is putting sensitive data on a removable media device such as an SD card or an optical disc and giving it to unauthorised parties (1)

(f) Eavesdropping a phone conversation (1)

(g) Maliciously accessing a financial server in order to falsify financial records (2)

(h) Maliciously erasing disk containing important information (2)

(i) Pushing an update to an app that modifies its permissions without notifying the users (2)

(j) Showing different users different views of the same web page --- could be seen as how you define attacks on the same system

(k) Sharing a patient’s medical record (or any sensitive data in other contexts) without their consent (1)

(l) Obtaining more data than necessary for the purpose of a task --- (1)

3. Are these (1) threats, (2) impact (i.e, harm) or (3) vulnerabilities? (justify)

(a) Thieves can enter the lab to steal equipment (1) (what could happen)

(b) Credit card numbers were stolen (2) (who is influenced)

(c) Users choose weak passwords (3) (where can the system break?)

(d) A backup system stopped working (3)

(e) A hacker can install malware (1)

(f) Students can see the exam questions before the test (1)

(g) A machine learning algorithm that is used to make important decisions is biased, or has a significant error rate (2)

(h) I am staying at a hotel that gave me access to my room without verifying my identity (3)

4. Is this a security problem? (justify)

(a) I need to send a wireless signal in an environment where there may be obstacles (walls, rain, ...) -- no

(b) I need to keep my valuable laptop in my car to go shopping -- yes

(c) I need to build a boat that floats under adverse conditions (storm) -- yes

(d) I need to store the secret final exam on a server open to the internet -- yes

(e) I need to make sure I am talking with my lawyer over the phone -- no

(f) I inadvertently added an infinite loop and took down my server -- yes

(g) My operating system offers full disk encryption, but really just uses the hard disk encryption mechanism – yes?

(h) I am connected to a public wireless network that does not seem to be encrypted -- yes

(i) I have sensitive information on my laptop/smartphone and have to go through strict border control -- no

(j) I cannot verify that the downloaded software comes from the intended software distributor -- yes

(k) My hardware and/or software is manufactured in a country that is hostile to my country

-- maybe

(l) I have lost my phone and it suspiciously reappears after some time -- no

(m) I am going to an event that has deployed facial recognition cameras – no

5. Consider the following situation: Los Angeles Unified School District started issuing iPads to its students this school year, as part of a $30 million deal with Apple. Now Sam Sanders reports at NPR that less than a week after getting their iPads, high school students have found a way to bypass software blocks on the devices that limit what websites the students can use. The students are getting around software that lets school district officials know where the iPads are, what the students are doing with them at all times and lets the district block certain sites, such as social media favourites like Facebook. ’They were bound to fail,’ says Renee Hobbs, who’s been a sceptic of the iPad program from the start. ’There is a huge history in American education of being attracted to the new, shiny, hugely promising bauble and then watching the idea fizzle because teachers were not properly trained to use it and it just ended up in the closet.’ The roll out of the iPads might have to be delayed as officials reassess access policies. Right now, the program is still in Phase 1, with fewer than 15,000 iPads distributed. ’I’m guessing this is just a sample of what will likely occur on other campuses once this hits Twitter, YouTube or other social media sites explaining to our students how to breach or compromise the security of these devices,’ says Steven Zipperman. ’I want to prevent a ”runaway train” scenario when we may have the ability to put a hold on the roll-out.’ The incident has prompted questions about overall preparations for the $1-billion tablet initiative.

Discuss how would you define the (1) threats, (2) vulnerabilities, (3) likelihood, (4) impact, and (5) protection in the above case?

1. Threats: