[TUTORIAL ONE]

1. **Which of the following terms describes the likelihood that a threat will exploit a vulnerability with a harmful result?** a) Risk b) Threat c) Vulnerability d) Countermeasure	Risk: The chance of an attack happening. Threat: Is the potential violation of security principles Vulnerability: A flaw or weakness of a design that could be exploited by an attacker Countermeasure: An action taken to prevent an attack
2. **Which principle of GDPR states that personal data must be collected for specified, explicit, and legitimate purposes?** a) Lawfulness, fairness, and transparency b) Purpose limitations c) Data minimization d) Accuracy	Lawfulness, fairness, and transparency: Gathering of data must be legitimate, transparent, and fair. Purpose limitations: You, as a data subject, have the overall control of your personal data. Data should NOT be used in ways unknown to the client. Data minimisation: No more data is collected outside of the scope of data collection purpose. Accuracy: Data is collected and stored, and must be done so correctly, and updated regularly.
3. **Which type of security attack involves the attacker impersonating another user or system to gain unauthorized access?** a) Replay b) Traffic Analysis c) Masquerade d) Denial of Service (DoS)	Replay: Hacker replays information to receiver. Traffic Analysis: Taking metadata, such as frequency, packets, time, etc Masquerade: Pretending to be someone else DoS: Overwhelming servers in an attempt to crash and prevent communication across services.
4. **Which of the following statements is true?** a) DoS attacks can be prevented by using robust antivirus software b) Cybersecurity ignores the involvement of the human aspect in the security process c) Network security is a subset of cybersecurity d) The main goal of a replay attack is to reduce the availability of resources	a) False because DoS attacks don't usually involve viruses, a better approach would be Content Delivery Network Services. b) False, Cyber security incorporates human factors such as email phishing. c) TRUE d) False, Hacker replays information to receiver. The main goal is to pretend to be the subject.
5. **Select the possible security vulnerabilities in a banking system.** a) Bank employees are unable to identify phishing emails b) The possibility of an attacker accessing unencrypted data in the bank database c) A bank customer uses a compromised password for online banking d) 1000 customers lose money due to unauthorised transactions	a) True, weakness in design in educating employees. b) False, this describes a risk. c) True, weakness in design in failure to ensure subjects under one entity's information must be secured. d) False, this describes an attack.
6. **What factors can be used to determine the impact of a security attack?** a) The amount of people affected by an attack b) The regulatory penalties incurred by an organisation due to an attack c) The number of attackers participated in the attack d) The sensitivity of the data items that were breached during an attack	a) True; EG: NZ census vs customer data from local sushi shop. The amount of people is a measurable impact. b) True c) False: 'impact' keyword, thinking about what happens after, what is the aftermath? d) True.
7. **What are the differences between cybersecurity and network security?** Cybersecurity focuses on protecting systems, networks, and data from digital attacks, theft, and damage. Network security is a subset of cybersecurity that specifically deals with protecting the integrity, confidentiality, and availability of data as it is transmitted across or between networks.	Cybersecurity protects against theft and damage for: - systems, networks, data Network security is a subset of cybersecurity, where is protects data: - integrity, confidentiality, availability
8. **How do the key changes in GDPR affect users and corporations?**	GPD (Previous policy before GDPR was imposed) only includes EU citizens living inside the region, while GDPR involves those living outside of EU locations.
9. **Explain the concept of 'Privacy by Design' as outlined in the GDPR. Describe its key elements and how it differs from traditional approaches to data protection.** The concept of 'Privacy by Design' in the GDPR emphasises proactive measures, embedding privacy controls into systems from the outset, ensuring end-to-end data security, and maintaining transparency with data subjects. This differs from traditional approaches which often address privacy reactively and integrate controls post-development, focusing on specific security points rather than the entire data lifecycle.	- Telling organisations to be proactive about privacy. - Acts as a simplified guide for a person who wants to serve regulations, GDPR policies are very lengthy, this shortens it. - Keep things by default, google always asks for permission for camera, audio, gallery, etc. So, tells us by default this setting should be set as NOT permissible.
10. **Analyse the cybersecurity attack reported in the following news article : Link.** **Answer the following questions.** a) What is the vulnerability that caused the attack? b) Which pillar of the cybersecurity triad is affected by the attack? c) Rate the impact of the attack and justify your answer.	a) IT security was inadequate and severely compromised. And a lack of training meant staff posed an unintentional threat. - Outdated systems including an OS being outdated for five years. b) Availability. Until victims paid, the hackers kept information for ransom. c) 4200 people were affected, with 6 months to recover, and more cost and time put into the organisation needing to recover, with surgeries being postponed and other repercussions. Relatively large impact. Can argue that this was 'medium' but you need to argue why it is NOT high. This would still classify as HIGH as medical information involves addresses, and very personal information.

[TUTORIAL TWO]

1. A system administrator notices an unusual spike in network traffic late at night, with data being sent to an unknown IP address. What type of malware might be most directly associated with this activity? a) Adware b) Ransomware c) Botnet d) Spyware	Adware: Pop-up advertisements with potential to be malicious upon clicking a link. Ransomware: A malware that prevents users from accessing software until the hacker is paid. Botnet: A group of computers taken over by malicious attack. Spyware: malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent
2. A company implements a new access control system that requires users to authenticate with a password and a fingerprint. This system is an example of: a) Single-Factor Authentication (SFA) b) Multi-Factor Authentication (MFA) c) Role-Based Access Control (RBAC) d) Biometric Authentication	SFA: Just using a password or pin, but no other authentication check is required. MFA: Multiple authentication procedures, such as confirmation email, another device, Touch ID, face ID, etc RBAC: Assigning permissions to users based on their role within an organisation Biometric: Using fingerprint, or biological related identifiers as a form of authentication.
3. A user reports receiving an email from an unknown source requesting login details for their company account. What type of attack does this represent? a) Man-in-the-middle attack b) Denial-of-service attack c) Keylogger installation d) Social engineering	MITM: Attacker gets in between you and system, you effectively communicate to attacker unknowingly. DoS: Overwhelming systems in attempt to crash servers and usually ask for a ransom. Keylogger: malware or hardware that keeps track of and records your keystrokes as you type Social engineering: Using psychological techniques to gain information or persuade humans.
4. What is the incorrect statement about the given list A, which shows what rights that the subjects (Bob, Alice) have regarding the object (file x)? List A => file x: ((Alice, read write), (Bob, read only)) a) List A can be extracted from a Access Control Matrix b) List A is a Access Control List c) List A is a Capability List d) Bob cannot edit the file x	A: Matix includes a list of users who have access to what file, and separately, a list of what permissions each user has. B: Yes, this is the AC list. C: Capability list would simply list what file each user is entitled to, and not their capability with such a file. D: Yes, Bob is unable to edit; he can only read.
5. What is/are the correct statement/s? a) A botnet is used to conduct a DoS attack, where a computer is used to flood a resource with traffic b) Social engineering is a malware that appears to be a legitimate resource c) A virus does not need user interaction to spread through a network d) Once a worm infects a device in a network, it spreads to all other devices in the network	A: True, botnets control many computers under one server in an attempt to run a DoS. B: False, not malware, it is using psychological tactics to manipulate a user. C: False. A virus is usually hidden in a clickable link. The virus needs to enter the OS or computer files in order to spread. D: True. Worms propagate or self-replicate without human interaction, enabling its spread to other computers across a network.

6.

Discretionary Access Control A: Some movies on Netflix are not allowed for the users who access Netflix from New Zealand

Mandatory Access Control B: The “nuclear missile launch” file is confidential and can be only accessed by the military officials who have the valid security level clearance

Role Based Access Control C: Lecturers do not have access to see the salary details of other employees, while HR personnel can access the salary details of other employees

Usage Control D: Ann and her brother both use the same computer with separate user accounts. Ann creates a folder named "My Images" and configures the folder's permissions to restrict access by other users

7. How does implementing the Principle of Least Privilege (PoLP) minimise the impact of a potential security breach in an organisation?

- There are less entry points for attackers.
- If a breach does occur, the damage can be contained to only those resources that the compromised account had access to.

8. What are the differences we can see when using hashing and encryption to protect passwords and which one is preferred for password security?

- Salt with Hash and Multi-factor authentication
- Salt with hash is preferred because if a user uses the same password for multiple sites, this can mitigate this vulnerability. This also makes offline dictionary attacks a lot harder to successfully conduct. MFA is also a good option, although this cannot mitigate the said vulnerabilities.

9. Explain the process of malware analysis and the role of sandboxing in detecting malicious behaviour.

- Malware analysis is the process of studying and understanding the behaviour, functionality, and origin of suspicious files or programs to determine their purpose and potential threat. The process typically involves two main approaches: static analysis and dynamic analysis.
- Sandboxing plays a crucial role in dynamic analysis by providing a controlled and isolated environment to observe the behaviour of malware

10. What are the typical signs that a computer may be affected by malware, and what steps should be taken to remove it?

- Changes in documents: this refers to document based malware where malware may override commands or send emails on your behalf. This can be mitigated through intrusion detection software, or phishing detection systems. Otherwise, simply educating users about email phishing or link malware.

[TUTORIAL THREE]

What role does user training play in usable security? a) It is unnecessary because usable security eliminates the need for user involvement b) It ensures that users understand and correctly use security measures c) It focuses only on technical aspects of security d) It guarantees that all users become cybersecurity experts	User training involves testing users, or having users attempt certain security measures. The role of user training is to gain insight on the extent of the usability of a security mechanism. The purpose of it, for programmers, is to measure how well people understand security mechanisms so they can either continue using these measures, or even decrease usability for a better security tradeoff.
A company has a web application where users can log in using their username and password. An attacker was able to manipulate the login form to execute unauthorised SQL commands, gaining access to sensitive user data. Which of the following measures would be most effective in preventing such an attack? a) Ensuring the application uses secure default credentials b) Implementing parameterized queries to separate user input from SQL commands c) Requiring users to create complex and strong passwords d) Configuring the application to handle XML data securely	In SQL, parameterise means we take an input from a user and assign the inputs to variables in a fetch/load instruction. Separating the input from the username/password database. Example of SQL injection SELECT * FROM userDataTable WHERE Name = "" or 1=1 AND Password = "" or 1=1
What is/are the reason/s that privacy concerns are often ignored during software development? a) Software developers' lack of knowledge in privacy related concepts b) Privacy concerns are trivial compared to functionality c) Privacy protection measures may require additional resources and effort d) Privacy regulations and guidelines are often complex and lengthy, making it difficult to understand them	- Ignorance to privacy policies - Little education given to programmers, so little thought given to privacy policies. - Complex privacy procedures to add into an already designed program. - Requires additional resources such as time, storage, computational power and money.
What is/are true statement/s regarding injection attacks? a) "Never trust user input", is a good injection prevention guideline for software developers b) Broken authentication is a type of injection attacks c) SQL injection attacks can only exploit web applications that accept user inputs d) A common way to detect injection vulnerabilities in web applications is to use a automated web vulnerability scanner	i. c ii. b,c iii. a,b,c iv. a,d v. All above
Which privacy threat is associated with "Zoom Bombing"? a) Data theft b) Unauthorized access and eavesdropping c) Malware installation d) Phishing attacks	Zoom bombing is when an unauthorised individual joins a Zoom meeting uninvited, gaining access to confidential conversations, information, data, etc.
Choose the vulnerability that best fits each scenario Cross Site Scripting (XSS) **A** XML External Entities (XEE) **B** Broken Access Control **C** Sensitive Data Exposure **D** Injection **E**	**A**→ An e-commerce website was hacked because an attacker exploited a vulnerability that allowed them to execute scripts in the browsers of other users **B** → An attacker compromised a web application by injecting XML content to access internal files and systems. **C** → During a security audit, it was discovered that an internal web application allowed users to escalate privileges and access administrative functions without proper authorization **D** → A healthcare provider's web application was found to be sending patient data over the network in plain text. **E** → A retail website experienced a security breach where attackers were able to execute commands on the server by submitting crafted input through a search form
"Separation of data from application logic" is an injection countermeasure. Explain the usefulness of this concept."	Separating data from application logic can be used to counter injection attacks and if someone can access the data, at least they cannot manipulate its inputs with its algorithm.
"Explain why usable security is important in cybersecurity"	To create a secure place for users while also having them understand and actually use the system under the security measures. This involves making security tasks, such as a password, easy to do, while effectively protecting information.
Sensitive data exposure is a critical issue in web security. a) Explain the types of data considered sensitive b) Discuss best practices for protecting sensitive data, providing examples of technologies and techniques used to achieve this protection.	a. Any information that relates to a person or an entity, personal information such as names, identities of individuals which may include addresses, financial data, transactions, etc. b. Passwords, authentication procedures, access control measures,

[TUTORIAL FOUR]

1	**A company is conducting a security review of its web application. They decide to use static analysis to inspect the source code for vulnerabilities before deployment. Which of the following benefits will the company most likely experience from using static analysis?** a) It will guarantee that no vulnerabilities exist in the code. b) It will reduce false positives by testing real-time inputs. c) It will ensure all potential execution paths are analysed without running the code. d) It will immediately fix vulnerabilities in the production environment.	Static analysis tests the possible paths of a program without reading it. a) Its purpose is to try to detect vulnerabilities by testing possibilities, so there is no guarantee of no vulnerabilities. b) Static analysis's main concern is its accuracy, when it becomes too particular, leading to identifying things that aren't actual vulnerabilities. c) TRUE d) Static analysis is just the first stage in risk assessment, it is just an observation/identification stage, hence there are no fixes.
2	**An e-commerce platform employs control flow obfuscation to protect its payment processing code. What is the primary objective of this approach?** a) To enhance the readability of the code b) To prevent attackers from easily understanding the logical flow of the payment process c) To optimise the performance of the payment processing d) To reduce the size of the executable file	Obfuscation is the process of making something unclear, such as a program to defer attackers or to mislead intruders. a) Obfuscation would actually decrease readability b) TRUE c) This would not be a security measure, more so some sort of efficiency/business operation d) The main goal is to confuse an attacker, not to preserve resources.
3	**An IT firm is developing a risk management strategy for its new product. Which of the following should be the first step in identifying the potential risks?** a) Performing continuous monitoring of the product b) Conducting a threat-vulnerability pair analysis c) Implementing intrusion prevention systems d) Creating a security policy for the product	The first stage of risk management is program analysis, in which the behaviour of a program is simply observed. Hence we can understand the types of threats or vulnerabilities before making some sort of threat/vulnerability analysis.
4	**What are true regarding software programs analysis?** a) Static analysis detects defects in the programs b) Dynamic analysis detects defects in the programs c) Static analysis detects failures in the programs d) Dynamic analysis detects failures in the programs	Both static and dynamic program analysis are measures to observe possible vulnerabilities in programs. Both of which identify defects and failures. Static does it by observing code without running the program, while dynamic works by running the program with different inputs. Dynamic analysis is more reliable in terms of accuracy as there is less of a chance of running into false positives due to the program being run in a real-time environment.
5	**What type of code obfuscation is this?** a) Layout b) Design c) Data d) Control	Layout: Hiding comments, debugging tips, and meaningful variable names Design: Merging classes, diving classes into smaller sectors, or revering classes as an attempt to make it difficult to follow a program. Data: Encrypting, splitting variables, or converting local/global variables Control: modifying if statements, or the control flow graph. An extra parameter is included, which is an example of variable splitting. Instead of using a and b directly, we use an obscure function.
6	**What is/are incorrect statement/s?** a) Mitigation techniques are needed to reduce vulnerabilities b) Mitigation techniques are needed to decrease the harmful impact of a risk c) Facebook server crashing can be an unintentional threat d) An identified threat alone can cause a risk to a company	a) TRUE: Mitigation can reduce vulnerabilities, for example if the company is vulnerable to losing data to an attacker, the mitigation technique 'version control' acts as a backup, so upon damage to files, they can be restored. b) TRUE: for example, implementation version control can decrease the cost of restoring expensive data, as well as time. c) TRUE: Unintentional threats are incidents that occur without malicious intent d) FALSE: An identified threat alone does not cause a risk to a company. For a risk to exist, there must be a combination of a threat and a vulnerability:
7	During routine security testing, dynamic analysis revealed a critical vulnerability in an e-commerce web application that was not detected by static analysis. Describe a scenario where this might occur and explain why dynamic analysis is more effective in this case	A web application has a feature that allows users to add items to their shopping cart and proceed to checkout. During routine security testing, dynamic analysis reveals a vulnerability where an attacker can manipulate the price of items in the cart by altering the values sent from the client side. Static analysis may miss vulnerabilities related to runtime behaviour, especially those involving user inputs that are processed dynamically.
8	A software developer who worked in a startup fintech company recently resigned. However, the company forgot to remove the developer’s access to its codebase. Describe two threats that can happen through the threat actor - the resigned developer. You can assume that the resigned developer has no intention to do changes to the code	They might unknowingly clone the repository onto a machine that is not secure, or upload the code to a public or shared repository by mistake. If the resigned developer's credentials are compromised, a malicious attacker could gain unauthorised access to the company's codebase.
9	A healthcare platform wants to secure its patient records by using data obfuscation techniques. a. Explain the concept of data obfuscation and how it can be applied to protect sensitive data within the application. b. Provide a scenario where data obfuscation prevents an attacker from extracting patient information. c. Discuss the potential drawbacks of this technique.	a. Making a program confusing or unreadable so attackers cannot clearly access it/read it/change it/clone it, etc b. An attacker tries to re-pack the code, but the engineer has implemented layout obfuscation, so upon checking variables, the attacker finds variables have confusing names, and cannot locate them properly or fast enough. c. Longer development time for the engineers, and may even confuse engineers when they are updating or reviewing their program.
10	Discuss how Static and Dynamic Analysis contribute to the overall software quality	The main purpose of program analysis is to review a code to identify possible vulnerabilities. With vulnerabilities identified, we can then think of different threats these vulnerabilities may pair with, and so mitigation techniques can be formed and implemented in order to safeguard a program, and prevent attacks or data loss.

[TUTORIAL SIX]

1	What is the primary goal of risk management in information systems? a) To eliminate all risks. b) To identify and mitigate risks to an acceptable level. c) To ignore risks that are deemed insignificant. d) To transfer all risks to third parties.	b) List risks, score them to identify low and high risks. More resources are given to high risk. We should do this within our own capabilities.
2	What is the role of the Fishbone Diagram in a cyber risk management plan? a) To outline the steps in a disaster recovery plan. b) To identify the root causes of specific risks within the organisation. c) To prioritise the implementation of security controls. d) To document the compliance requirements of the organisation.	b) A fishbone diagram is a framework that helps find all possible causes of risk. Above the arrow, we outline threats, and under the arrow, we outline vulnerabilities. Ofcourse, a risk cannot exist without the pair, hence this framework helps to observe threat-vulnerability pairs.
3	Which of the following is a real-world application of STRIDE in risk management? a) Calculating the potential financial loss due to a cyber attack. b) Ensuring compliance with international data protection regulations. c) Conducting physical security assessments for office premises. d) Identifying and addressing specific software vulnerabilities in a newly developed application.	d) In STRIDE, we only identify, although the working 'addressing' is incorrect, a better word would be identify.
4	Why is it important to conduct a cost-benefit analysis (CBA) when selecting controls for risk management? a) It ensures that the organization achieves the highest level of security, regardless of cost. b) It guarantees compliance with industry-specific cybersecurity frameworks. c) It helps prioritize controls based on their potential to reduce risks and their associated costs. d) It helps in identifying the most vulnerable aspects of the organization's cybersecurity defenses.	c) Controls are mitigations. CBA occurs before we implement action, and it helps us decide on which tools or paths to take before actually taking them.
5	What is/are incorrect regarding disaster recovery plan (DRP)? a) Reduced recovery cost is a benefit of having a DRP. b) Having a DRP is useful in getting cyber insurance. c) It is done before threat modelling. d) A good DRP help companies get back up and running swiftly and smoothly after an unplanned security breach	i. a (True, a DRP is a plan that foresees future risks) ii. a,b (True, Insurance companies need to see a DRP before giving you a service) iii. a,b,d (True) iv. c (DRP comes after, not before threat modelling) v. none
6	Revisiting a security threat model and updating it accordingly is advisable after which event(s) out of the following a) Changing the database architecture from relational to non-relational b) A new feature is introduced to a existing trading application c) A security breach occurs d) A company changes the logo of their software products	i. a ii. a,b iii. a,b,c iv. a,b,d v. all above a, b, and c listed events may cause new vulnerabilities, meaning we need to iteratively review the security threat model.
7	What is the significance of identifying both in-place and planned controls during a risk assessment?	In-place controls help to control processes, training, insurance, etc right away. This is useful for when there is an existing risk. Planned control helps to mitigate risk that could happen in the future, they usually entail some sort of start and due date, with carefully thought out resources, details, and documentation, these plans can mitigate bigger risks or foreseeable risks.
8	Explain the importance of documentation in cybersecurity risk management.	Documentation is important so the company can look into historical changes, or make improvements from past events. It is also helpful to have management and teams on the same page. It enables well-informed decision and communication internally.
9	Imagine you are working as a cybersecurity consultant for a healthcare organisation that is about to implement a new electronic health record (EHR) system across all its hospitals and clinics. Given the critical importance of patient data security and regulatory compliance, what are the fundamental components of an effective risk management plan that you would develop to ensure the security of the EHR system?	1. First start by listing threats and vulnerabilities to identify. 2. Observe threat-vulnerability pairs, risk does not exist without a pair. 3. Create a cost-benefit analysis and evaluate dimensions of risk weighting 4. Ensure that compliance issues are also mitigated 5. Develop the mitigation techniques, this involves conducting business impact analysis, disaster recovery plans, etc 6. Send this analysis to the manager and update the POAM (document) 7. Create a GANTT chart or something to show the project schedule 8. Use the chart to track risk management mitigation
10	You are working on a risk assessment for a company's IT infrastructure, which includes three critical components: an internal financial system, a public-facing website, and an employee email system. Each component has different values for threat likelihood, vulnerability severity, and asset importance. a. Calculate the risk for each component b. Rank the components from highest to lowest risk based on calculations c. Discuss the implications of these rankings for prioritising risk mitigation efforts.	Risk = Threat * Vulnerability * Asset Internal Financial System = 7 *5*9 = 315 Public-Facing website = 5*7*6 = 210 Employee Email System = 4 * 3 * 7 = 84 Highest Risk: Internal financial system Middle Risk: public facing website Lowest Risk: Employee email system In this case, of course we would have to prioritise internal financial systems as it has the biggest risk. While we would then focus on public facing websites, and finally employee email systems.

[TUTORIAL SIX]

1

What is/are the correct statement/s?

- a) Pseudonymised data are governed by GDPR.
- b) “Visibility and Transparency” in privacy by design means informing developers about data handling practices of their products.
- c) “Data Privacy” is only about protecting personal data
- d) K-anonymised data are governed by GDPR.

i. a
ii. a, b, d
iii. a, c
iv. a, d
v. c, d

- a) Pseudonymised data is still at risk of re-identification, GDPR protects anonymised data, but not de-identified data. Hence, GDPR still governs data that is pseudonymised and k-anonymised.
- b) This concept describes the empowername of data subjects and how they are entitled to knowing what, where, how etc their data is being collected and used, and not necessarily the handling of it.
- c) Data privacy also includes how it is handled, stored, accessed, governed etc.
- d) Refer to a

2

What is incorrect regarding PETs?

- a) Every PET is not suitable for practical implementations.
- b) Synthetic data can be used to train machine learning models.
- c) Scalability of PETs is considered when selecting them for privacy protection.
- d) Applying PETs will prevent Ransomware attacks

- a) True because of scalability and cost / resource limitations
- b) True
- c) True
- d) false: PETs are more concerned about protecting privacy, but PET-transformed data can still be stolen and sold for a ransom

3

What is true regarding Pseudonymisation?

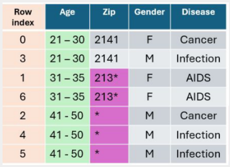
- a) Pseudonymisation always generates a mapping table.
- b) Counter is the only way to generate pseudonyms.
- c) Pseudonymisation is a naive PET
- d) Pseudonymisation removes the link between individuals and personal data.

4

What are the correct statements regarding the privatised table?

- a) It satisfies 2-Anonymity.
- b) It satisfies 3-Anonymity.
- c) The Mondrian algorithm can be used to achieve the row partitions [0,3], [1,6], [2,4,5].
- d) Preprocessing data might be applied before achieving the given outcome.

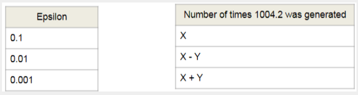
i. a
ii. b
iii. a, c
iv. a, c, d
v. c, d



Row index	Age	Zip	Gender	Disease
0	21 – 30	2141	F	Cancer
3	21 – 30	2141	M	Infection
1	31 – 35	213*	F	AIDS
6	31 – 35	213*	F	AIDS
2	41 - 50	*	M	Cancer
4	41 - 50	*	M	Infection
5	41 - 50	*	M	Infection

5

Query: “What is the total number of people in the dataset”.
This query was executed on dataset D. The real answer is 1000. But when differential private results were generated for epsilon values 0.1, 0.01, 0.001 one possible noisy result that was achieved is 1004.2. Suppose X and Y are greater than 0. Match the possible number of times 1004.2 was generated under each epsilon when the query was executed multiple times.



Epsilon
0.1
0.01
0.001

Number of times 1004.2 was generated
X
X - Y
X + Y

0.1 → X + Y
0.01 → X
0.001 → X - Y

The bigger the epsilon (noise), the smaller noise, and closer to true value. The smaller the epsilon (noise), the more noise and further from true value.

Hence, the biggest e is 0.1, so it should generate 1004.2 most frequently, which is why X+Y. 0.001 is the smallest e, so it generates 1004.2 less frequently.

6

What is/are the correct statement/s regarding Differential Privacy?

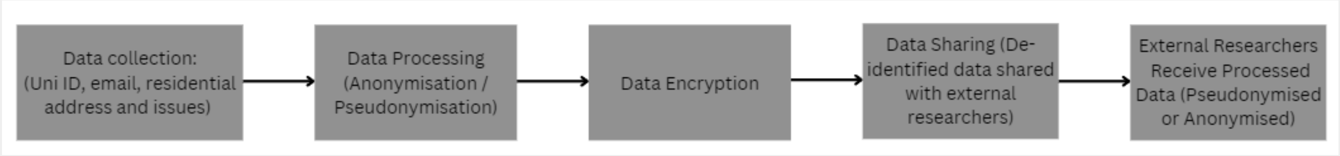
- a) Privacy guarantee of a differentially private result is lost by post-processing it
- b) It can be used to mitigate non-repudiation threat
- c) Differentially private query results are randomised
- d) By using it we try to reduce the distinguishability of an individual included in a datasets

i. b. c
ii. a, d
iii. a, b, c
iv. c, d
v. b, c, d

7

Q1: Bundoran Way (3, 6, 5 OR 8)
Q2: He studies at UoA, specifically, OGGB, General Library, and Science building, he takes the Albany bus to get there. He has visited New World, Event Cinemas, Woolworths, KFC, and the address 36-36 Mandeville Place.
Q3: Uber, it looks like he uses public transport alot. Wespac shopping centre, and KFC
Q4: Most commonly travelled to places, where family members / friends might live, his workplace, etc

8



Data collection: (Uni ID, email, residential address and issues) → Data Processing (Anonymisation / Pseudonymisation) → Data Encryption → Data Sharing (De-identified data shared with external researchers) → External Researchers Receive Processed Data (Pseudonymised or Anonymised)

Threat 1: Unauthorised Data Access (Disclosure of Information) Even with encryption, there's risk that unauthorised parties gain access to sensitive information
Threat 2: Re-identification Risk (Identifiability) If data is pseudonymized but not fully anonymized, there's a risk that researchers or third parties could potentially

	re-identify individuals based on patterns or other indirect identifiers in the data. Threat 3: Data Leakage During Transfer (Disclosure of Information) Data could be intercepted or accessed during transmission between the university health centre and external researchers if secure transmission protocols are not properly implemented.