# SIT223/753 - Task 1.2P - Answer Sheet

**Cybersecurity Case Study: The Insider Threat Data Breach**

1. Weak employee monitoring : The company should monitor and track every single employees activity in order to prevent from data breaching. The organisation should prohibit the use of unknown USB's or any kind of drivers for that matter.

2. The TechFinance Ltd could have prevented this type of insider attack by simply implementing some kind of dual protection system before letting employee access the data. They could also have added the dual factor authorisation by which the employee would have got caught while manipulating company's private data.

3. Under the Australian Privacy Act & APPs, TechFinance Ltd. must secure personal data and notify affected customers when a serious breach occurs.

4. Yes, I believe the company should inform the customers irrespective of how much the information is available. They should take full responsibility for the misconduct and provide time-to-time updates.

5. They should form strict rules and regulation for those employees who breach the code of conduct and keep track on logs.

**Ethic Case Study: Data Sharing for Targeted Advertising**

1. Gamers agreed to share data for game improvements and user experience, not for selling data. Players don't have clear consent for third-party data sharing.

2. Gamers' privacy and trust: They expect fair use of their data. Selling data can by profitable but could harm reputation so breaching privacy laws could lead to lawsuits.

3. The possible consequences of the actions taken by the individuals can involve stopping to use the game or file complaints. Ask the organisation to remove their personal data from their database

4. Yes, Guidance from ACS Code of Ethics include Honesty, Privacy: Protect user data from misuse and make sure Developers should ensure their work doesn't harm users.

5. alternative approaches or actions includes -
   a) Limit Permissions for the game
   b) opt-out options
   c) Guest signing only
   d) Limit background recording
   e) Stop in app purchase
   f) No social media authentication(Google, Facebook, Instagram, GitHub)
   g) Gain explicit consent
   h) options for rejecting cookies