PROSEC PDPA CODE OF CONDUCT

You must make sure that the personal data collected in your assigned premises is Accurate, Protected and Retained according to our Data Protection Policies.

1. Daily Deployment Routine

- You must record the vehicle and driver particulars accurately
- You must protect and keep the vehicle and driver particulars in a safe place that is away from public view
- You must record personal information accurately during incident handling and post-incident follow ups
- You must protect and keep the incident handling and follow up records in a secure place
- You must keep your pocket book with you at all times
- You must surrender the completed log book, follow up records and pocket book to your CSO
- You must not speak about the personal data of visitors in front of other visitor
- You must not reveal any personal data to unauthorized persons

2. Handling of Personal Data during Visitor Registration

- You must inform all visitors our purpose for ID collection i.e. security, safety and verification purposes
- You must check the identity of all visitors and ensure they sign in
- You must check that all personal data collected is accurate
- You must not expose the recorded personal data to other visitors
- You must protect and keep visitor personal data and hardcopy ID in a safe place that is away from public view
- You must verify the photo and name on the ID before returning the ID to visitor
- You must not allow a third party to collect the visitor's ID unless a written permission is given by the ID owner
- You must logout of the Visitor Management System (VMS) when not in use
- You must not speak about the personal data of visitors in front of other visitor
- You must not reveal any personal data to unauthorized persons
- You must make sure that only staff on duty are allowed to enter the guardhouse / reception counter

3. Management of CCTV Footage

- You must make sure that all the CCTV footage is protected and stored in a secure location
- You must make sure that the CCTV equipment is secure at all times
- You must make sure that the CCTV footage is encrypted where practicable
- You must make sure that monitor screens are kept away from public view
- You must make sure that only authorized personnel in the company can have access to the CCTV footage

- You must not take photo or do video recording of the CCTV footage from the monitor screens and post them on social media or forward to family and friends
- When a member of the public requests for CCTV footage, you must inform your CSO. Your CSO will handle the request according to the company's data protection policy and SOP
- You must make sure that the CCTV footage is destroyed at the end of its retention period or overwritten by new video footage

4. Management of Bodycam Surveillance

- You must use the bodycam with caution as they are highly intrusive to the privacy of individuals
- You must inform the members of the public that you have a bodycam and ask for permission to switch it on
- You must explain to members of the public why you need to switch on the bodycam
- In the case of criminal activities or intention, you do not have to inform nor ask for permission on the use of the bodycam
- During surveillance patrol or surveying crowd behaviour, you do not have to inform nor seek permission on the use of the bodycam
- You must use the bodycam only for the original purposes according to the SOP
- You must store the bodycam images in a secure location
- You must switch off the bodycam and keep it securely when not in use
- You must make sure that the audio/video data recorded by the bodycam is encrypted where practicable
- You must make sure that only authorized personnel in the company can have access to the bodycam images
- You must make sure that the bodycam images are destroyed at the end of its retention period or overwritten by new video footage