

STANDARD OPERATING PROCEDURE (SOP)

23-10-2025

Title: Bus Entry/Exit Security Check using Face Detection Devices

1. Purpose

This SOP explains the step-by-step process for verifying employee gate passes using face detection devices installed in buses entering and exiting SEEPZ premises.

2. Scope

This SOP applies to:

- i. ADC (Security)
- ii. Gate In-Charges
- iii. Security Guards / Head Guards
- iv. Private Security Personnel
- v. Units operating buses for employees
- vi. VAMS Team and IT Section

3. Roles and Responsibilities

3.1 Units

- i. Provide face detection devices to the bus operators and ensure that the device shall be mounted in bus.
- ii. Addition and deletion of the employee data will be managed by the units through their respective Pravesh admin login.
- iii. Immediately inform the Security Section if any employee is unable to scan their face, so their data can be uploaded.
- iv. Inform the Security Section about the names of units sharing the same bus.
- v. Data enrolment in face detection devices shall be maintained **unit-wise**. Each unit shall ensure its employee data is updated through the Pravesh admin portal at least two days before the employee begins using the bus service.
- vi. Coordinate with VAMS and Security Section for regular face data updates in devices.
- vii. Ensure that all employees availing the bus service of their respective units have been informed to mark their attendance on the device installed in the bus before arrival at and departure from the SEEPZ premises.
- viii. Units shall ensure that their employees are informed to self-declare if they are occasional users of the bus service and their data is not available in the face detection device installed in the bus.
- ix. Units shall inform employees that they must not get off the bus while the security guards are checking the bus or before the check is completed.

3.2 Bus Owners / Operators

- i. Ensure that the face detection device is installed at a proper height for easy scanning.
- ii. Make sure all passengers scan their faces before the bus starts.
- iii. Only employees of the declared units should travel in the bus.
- iv. If any other employee boards, inform the Gate Security Guard so attendance can be marked manually.
- v. Bus operator shall not share the attendance.
- vi. The device must always be installed on the bus upon arrival at and departure from the SEEPZ premises.
- vii. Make sure that the device should be mounted at the place where employees can easily mark attendance without touching the device by co-ordinating with M/s Vams team.
- viii. Buses will remain fixed for units according to the bus number.

- ix. Separate login will be provided to Bus Owners/Operators, enabling them to assign each bus to one or multiple units as applicable.
- x. Bus Owners shall ensure that there is adequate lighting inside the bus to avoid any issues during night-time operations.
- xi. Drivers shall be informed that the device must be fully charged and functional to display scanned details. If the device is not operational, the bus will not be allowed entry into SEEPZ, and employees will be required to use the pedestrian entry gate by scanning their QR code.
- xii. Bus owners shall ensure that their bus drivers be informed that the devices will auto sync every day between 12:00 am to 05 :00 am which will add/deleted the latest updated data and also make sure that the device may be charged or in proper network with good speed.

3.3 VAMS Team (System Integrator)

- i. Deliver devices to the concerned units within 2 days of order placement.
- ii. Load the device with data of all employees of the relevant units.
- iii. Make sure that the attendance marked by the units employees shall be automatically shown on screen of attendance, with no manual intervention required.
- iv. Ensure auto-synchronization of data across all buses or provide a feature to fetch data by Unit Name from the server.
- v. Provide the add/delete option in units login for the employees travelling by bus.
- vi. The bus device should allow selection of a unit (or group of units) to fetch relevant employee data. Ensure that training is provided to the concerned units on how to do this.
- vii. Inform ADC (IT) and ADC (Security) immediately if any implementation issue occurs.
- viii. Ensure that the system sends automatic reports to the admin (Security Section) every 2 minutes and to units with both the match and unmatched details.
- ix. Provide daily matched/unmatched face reports and a monthly dashboard to units showing employee-wise bus usage frequency.
- x. There shall be no requirement for the security guard to press any button on the device. The guard shall receive the report automatically on his tablet. However, until this functionality is developed and deployed, the existing mechanism shall continue, and each bus trip shall be considered complete only after the guard clicks the "Share" button once the bus enters or exits SEEPZ.
- xi. The VAMS Team shall physically inspect all mounted devices to ensure proper installation and accurate attendance marking by employees.
- xii. The bus contractors shall ensure that all devices installed in buses are properly mounted on stands and are functioning correctly after installation.
- xiii. The VAMS Team shall ensure that unit administrators and bus contractors are adequately trained on the features and operation of the application to enable smooth and uniform implementation.

3.4 Security Section

Role	Responsibilities
A. Assistant Development Commissioner / Security Officer	(i) Collect daily attendance and verification reports. (ii) Coordinate with the IT Section and VAMS Team for resolving device or data issues. (iii) Monitor the overall process and ensure timely issue resolution.
B. Gate In-Charge	(i) Compile daily reports in the prescribed format based on guard data. (ii) Immediately inform ADC (Security) of any discrepancy, device malfunction, or process failure.

	(iii) Report any inconvenience faced by unit employees and ensure smooth bus entry and exit. (iv) The Gate Incharge must ensure that they arrive half an hour before the shift and provide proper briefing to the security guards.
C. Head Security Guards / Security Guards	(i) Supervise private guards during bus checking. (ii) Coordinate with Gate In-Charge and Private Security Guards for attendance verification and record keeping.
D. Private Security Guards	(i) Check face detection data and compare it with the actual number of passengers. (ii) If total (Matched + Unmatched) equals actual passengers, send report to Admin through the bus tablet. (iii) If counts do not match, ask unmarked passengers to mark attendance at the pedestrian queue before allowing the bus to proceed.

3.5 IT Section

- i. Coordinate with VAMS to identify and resolve any system or software issues.
- ii. Handle all technical troubleshooting and report findings to ADC (IT) and ADC (Security).

4. Procedure

4.1 Employee Boarding and Attendance (Before Entry/Exit):

- i. Before the bus enters or exits SEEPZ, all employees must scan their faces on the bus-mounted device.
- ii. The system will display the result as:
 - a. **Matched:** No further action required.
 - b. **Retake:** Retake the scan. If still unmatched, inform the Unit Admin, who will coordinate with the Security Section for data update.
 - c. **Unmatched:** Immediately inform the Unit Admin, who must get the employee's face data updated through the Security Section at the earliest.

4.2 At SEEPZ Entry/ Exit Gate:

- i. When the bus arrives at the gate, the security guard shall scan the **bus pass** and the **driver's pass**, and verify the attendance on his **tablet/device** for that specific bus. The guard shall ensure that the **security check is completed efficiently and in minimum time** by adopting practical methods, such as:
 - a. Counting **vacant seats** when the number of empty seats is fewer (as the total seating capacity of the bus is already known), or
 - b. Counting **occupied seats** when the number of passengers is fewer.
 - c. The guard shall then verify that the **total number of occupied seats corresponds to the attendance marked** in the device. Once the verification is complete, the bus may be allowed to proceed.
- ii. The screen will show:
 - a. Authorized/Recognized faces (marked "Present").
 - b. Unknown faces (not recognized by the system).
- (ii). Physically verify any unknown person:
 - c. If unauthorized/ unmatched (ask them to allow access through pedestrian queue).

- iii. Security guards shall not check each visitor of the bus individually; however, they shall conduct random checks of buses to ensure that only those visitors who have marked attendance are travelling and that no unauthorized person is on board.

Note: If any such unauthorized person is found, the security guard shall immediately inform the ADC (Security), who shall take appropriate action with the approval of the Competent Authority.

5. Exception Handling:

Scenario	Action
Device not working	Report immediately to VAMS and Security Supervisor. Use manual attendance log until resolved.
Data not transferring	Retry data sharing, check network/device status, and raise issue with VAMS.
Unauthorized person found	Stop entry/exit, record details, and inform ADC (Security).

6. Compliance: Following this SOP is mandatory for all concerned personnel, and any deviation from the prescribed procedure must be immediately reported and properly recorded.

This SOP is issued in accordance with the decisions taken during the meeting held on 13.10.2025.

(Mital Hiremath)
Joint Development Commissioner
SEEPZ SEZ, Mumbai