LAHORE SECURITY / FIELD HANDBOOK

Access Control Guard Playbook

A practical guide to managing physical entry, visitors, vehicles, records and unusual situations at a guarded post.

START HERE

Every assignment has its own written site instructions. Confirm who can authorise entry, which ID checks are allowed, how exceptions are handled, and whom to contact in an emergency before taking the post. This guide supports those instructions; it cannot grant powers or permissions.

USE THIS PLAYBOOK FOR

- Reception desks, apartment entrances, office gates, loading points and event entrances.
- New-guard orientation, supervisor briefings and shift handovers.
- A simple, consistent process when a person or vehicle requests entry.

CORE RULE

Check identity. Confirm permission. Apply the correct site procedure. Record what matters. Escalate uncertainty. Keep emergency exits usable.

Prepared for LahoreSecurity.pk | 25 September 2026

01 Understand the assignment

Physical access control determines who may enter, where they may go, and when they may enter. A guard applies the site rules at doors, gates and checkpoints. A card, QR code or biometric device can assist, but the guard still handles exceptions, visitors and suspicious activity according to instructions.

Know the five questions before your first entry

Question	What to confirm with your supervisor
Who?	Approved staff, residents, visitors, contractors and delivery personnel.
Where?	Public, staff-only and restricted areas; escort requirements.
When?	Opening hours, shifts, appointment windows and after-hours rules.
How?	Approved credentials, ID check, host confirmation and register.
Who decides exceptions?	Named supervisor or authorised site representative and a working contact number.

Your authority has limits

• Follow documented site instructions; never invent an exception because a person is senior, familiar or in a hurry.

• Do not search people, bags, phones or vehicles unless the assignment explicitly authorises a lawful, defined procedure and you are trained to use it.

• Do not keep anyone's original identity document unless a lawful, approved site procedure requires it. Avoid taking photos of ID on personal devices.

• Do not physically confront, chase or detain someone merely because entry is disputed. Seek help and follow the site incident plan.

> **Simple decision**
>
> No verified permission means no routine entry. Pause, contact the authorised person, and document the result. If there is an immediate threat or medical emergency, activate the site emergency procedure.

02 The standard entry sequence

Step	Guard action
1. Pause & greet	Stay at the post. Ask for the person's name, purpose and destination without publicly announcing private details.
2. Verify identity	Check the site-approved badge, pass or identity evidence. Look for obvious mismatch or expiry; do not assume a uniform is proof.
3. Confirm authorisation	Check the approved list, appointment, resident or host approval, access system and permitted area/time.

Step	Guard action
4. Apply site conditions	Follow any required sign-in, temporary pass, escort, vehicle or delivery procedure.
5. Allow or refer	Admit only to the approved area; if the check fails or is unclear, keep the entrance secure and refer to the named contact.
6. Record & observe	Log required entry details and exceptions; check that the barrier closes and no unauthorised person follows.

03 People: staff, residents and visitors

Employees and residents

• Use the credential or approved recognition process required by the site. Check the area and time privileges when relevant.

• For a missing, borrowed, damaged or expired card, use the written fallback procedure. Do not lend out a master card or share a PIN.

Visitors and contractors

• Confirm the appointment or request approval from the host through an approved contact channel. A visitor naming an employee is not by itself authorisation.

• Capture only the register fields required at your site, such as name, organisation, host, purpose, arrival/departure time and pass number.

• Issue a visitor pass if required; tell the visitor where they may go and whether an escort is needed. Record pass return at exit.

• For maintenance work, verify the work order, authorised area, hours and escort or permit requirements with the site contact.

A professional explanation when you must wait

> **Suggested wording**
>
> “I need to confirm your access with the site contact before I can let you through. Please wait here while I check.”

04 Vehicles, deliveries and busy entrances

Vehicles and drivers

• Confirm driver identity and purpose, vehicle plate, destination and expected delivery or collection where the site requires it.

• Use the approved parking/loading route. Keep pedestrian paths clear; never stand directly in front of a moving vehicle or beneath a barrier.

• At a barrier, allow one authorised vehicle at a time where safe and feasible. Report attempts to follow another vehicle through.

Packages and couriers

• Confirm the recipient or receiving department and follow the site's delivery acceptance and package-handling policy.

• Keep deliveries in designated areas. Record receipt or refusal when required; do not sign for goods you cannot accept under site rules.

Queues and high-traffic periods

• Never skip authorisation checks simply to shorten a queue. Ask for relief or an additional officer if the assigned procedure cannot be performed safely.

• Use a clear waiting position and preserve a route for emergency responders and evacuation.

05 Tools, credentials and records

Control	Guard responsibility
Manual register	Write accurate times and factual observations. Store records so unauthorised people cannot read them.
Temporary pass	Issue only under approved authority; record number, permitted area and return or cancellation.
Card, PIN, biometric reader	Check whether the system grants the required zone/time. Do not override a denial without approved authorisation.
Turnstile or gate	Observe passage and closure; do not bypass safety features or block an emergency exit.
CCTV / alarm	Use only assigned equipment; respond to alerts under the site response plan and report faults.

Protect visitor information

Registers may contain personal details. Keep paper logs away from public view, use only approved systems, and follow the site retention and disposal instructions. Share entries only with authorised staff. Do not post incident or visitor photos on social media.

If the system fails

Keep the checkpoint supervised. Inform the supervisor or control room, record the fault and time, and switch only to an approved fallback, such as manual verification plus a controlled register. If there is no approved way to verify a request, do not improvise access. Restore normal procedure only after authorisation and document the changeover.

06 Denied entry and incidents

Situation	Immediate response
No appointment / unknown person	Ask the person to wait in the designated place; contact host or supervisor; do not reveal restricted information.
Credential rejected	Check expiry, zone and obvious reader fault; use the approved fallback or escalate.

Situation	Immediate response
Tailgating attempt	If safe, ask the person to stop and return to reception. Do not pursue into restricted areas; report location and description.
Person becomes aggressive	Maintain distance, avoid argument, call support, protect others and follow the escalation plan.
Suspicious item or activity	Do not touch or investigate beyond training. Move to safety, report promptly and follow site emergency instructions.

A useful incident note

Record date and exact time, checkpoint, people or vehicle involved (only necessary details), what you directly observed, what you did, whom you notified, and the outcome. Separate observation from assumption. Preserve related records according to supervisor instructions.

07 Emergencies and shift handover

Fire, medical emergency or evacuation

Raise the alarm and contact the designated response team or emergency services as the site plan requires. Follow the site's evacuation and muster procedures. Help direct people only within your assigned training and role. Do not lock, obstruct or improvise a change to an escape route. Confirm how access barriers and door releases behave in a power failure before an emergency occurs.

Shift handover: tell the next officer

- Current access rules, temporary changes and contact numbers.
- Expected late visitors, contractors, deliveries and their approval status.
- Outstanding passes, keys, badges, vehicles and equipment faults.
- Unresolved access denials, incidents and supervisor instructions.
- Register location, emergency routes and any post that must remain covered during relief.

Handover confirmation

Outgoing officer: _____ Incoming officer: _____ Date/time: _____

08 Ready-to-use post checks

Start-of-shift check

- [ ] Site instructions and contact list available
- [ ] Door, gate and emergency exit status understood
- [ ] Reader, radio, CCTV and alarm status checked
- [ ] Passes, register, keys and approved forms accounted for
- [ ] Expected visitors and restrictions reviewed

Per-arrival check

- [ ] Identity checked using approved method
- [ ] Permission, destination and time confirmed
- [ ] Sign-in, pass and escort completed if required
- [ ] Entry recorded and barrier closed

End-of-shift check

- [ ] Exceptions and incidents written up
- [ ] Unreturned passes and keys reported
- [ ] Open access requests handed over
- [ ] Equipment faults and emergency concerns passed on

Quick examples: apply the rule consistently

Scenario	Good guard response
“My manager told me to come in.”	Ask for identification and verify with the authorised manager using the approved contact details.
Employee forgot a badge.	Follow the missing-card procedure; confirm identity through approved means; record the temporary access.
Courier asks to enter a staff-only floor.	Confirm delivery point. Keep them in the permitted receiving area unless authorised escort/access is arranged.
An unknown person follows a resident through a gate.	If safe, challenge from a secure position; do not physically block or chase; alert supervisor and log the event.
Card reader is down.	Notify control room; use the approved manual procedure; document start/end of outage and each exception.

Common terms

Credential: an approved pass, badge, token or other means used to identify or authenticate a person. Authorisation: permission to access a particular place at a particular time. Tailgating: following an authorised person or vehicle through a controlled entry without independent approval. Escort: an authorised person who accompanies a visitor where the site requires it. Exception: an access request outside the normal process that must follow the documented escalation route.

Sources and scope

This training aid adapts general physical-security guidance; cited US and UK sources are operational references, not statements of Pakistani law. Local site instructions, employer policy and applicable Pakistani requirements govern each assignment.

NPSA - Control Access

NPSA - Automatic Access Control Systems

CISA - Facility Access Control

NPSA - Perimeters and Checkpoints

OSHA - Emergency Action Plan Elements

ICO - Records Management and Security