JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Physical Access Control Systems Training Course for Security Supervisors

26 – 30 September 2027
Cairo

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Physical Access Control Systems Training Course for Security Supervisors

Ref: 2448_92482 **Date:** 26 – 30 September 2027 **Location:** Cairo **Fees:** 3500 GBP

Physical Access Control Systems is a 1-week training course for security and facilities supervisors who run credentials, readers, zoning and visitor entry, and who leave with a Site Access Control Plan. As sites mix contractors, shift workers and visitors, every door decision now shapes safety, insurance exposure and staff trust. The course is offered by Jupiter Prime Training.

Why Physical Access Control Systems Matter Now

Three forces shape physical access control today: networked door controllers that turn every reader into an IT asset, a workforce of contractors and temporary staff whose rights change weekly, and insurers and auditors who ask for evidence of who entered where. A well-run system shows a clean audit trail after an incident; a poorly run one carries orphaned cards and propped doors. The course rests on international electronic access control performance requirements and on the principle of least privilege.

Who Gains Most from Physical Access Control Systems

- Supervisors who issue, suspend and recover cards, fobs and PIN credentials
- Control room leads who acknowledge door-forced and door-held alarms
- Facilities supervisors who own door hardware, locks and fire-exit interfaces
- Reception and front-desk leads who register visitors and contractors
- Shift leads who run patrols and check zone boundaries out of hours

The gain is greatest when a security lead and a facilities lead from the same site attend together, because door hardware and access rights then share one owner.

Physical Access Control Systems Capabilities

Participants work with credential records, alarm queues and event logs to make defensible door choices.

- Design a zoning map that groups doors by risk and occupancy — site manager and insurer
- Specify credential types and issue rules for staff, contractors and visitors — HR and procurement
- Build access-level templates that apply least privilege by role — department heads
- Apply an alarm triage routine for forced, held and tailgating events — control room team
- Test audit trail reports against a sample incident question — auditors and investigators
- Communicate a periodic access recertification cycle to line managers — compliance owners

Key Physical Access Control Systems Terms

- Credential — the card, fob, mobile token, PIN or biometric template a person presents to a reader to claim an identity.
- Access level — a named set of doors and time schedules assigned to a group of credential holders.
- Anti-passback — a controller rule that refuses a second entry until the credential has been recorded leaving the zone.
- Door-held alarm — an event raised when a door stays open longer than its configured shunt time after a valid entry.
- Fail-safe and fail-secure — lock behaviours on power loss: fail-safe releases the door, fail-secure keeps it locked.
- Access recertification — a scheduled check in which managers confirm or remove each person's door rights.

Physical Access Control Systems Day by Day

Day 1: Site Risk and System Architecture

- Site Threat and Asset Survey — Which Areas Need Controlled Entry
- Controller, Reader and Lock Architecture — Where Decisions Are Made at the Door
- Access Control Security Grades — Matching System Grade to Site Risk
- Fire Egress and Life Safety Interfaces — Balancing Exit Safety Against Entry Control
- Networked Controller Exposure — Coordinating Door Systems With IT Security Owners

Day 2: Credentials and Zoning

- Credential Technology Comparison — Choosing Cards, Mobile Tokens or Biometrics
- Credential Life Cycle Procedure — Issue, Suspension, Loss and Recovery Rules
- Zoning Map and Perimeter Layers — Grouping Doors by Risk and Occupancy
- Access Level and Time Schedule Templates — Applying Least Privilege by Role
- Anti-Passback and Tailgating Controls — Deciding Where Strict Entry Rules Pay Off

Day 3: Visitors, Contractors and Access Policy

- Visitor Registration and Host Escort Rules — Who Vouches for Each Guest
- Contractor Temporary Access Profiles — Limiting Rights to Job and Duration
- Written Access Control Policy — Setting Ownership, Exceptions and Sanctions
- Joiner, Mover and Leaver Triggers — Linking HR Changes to Door Rights
- Master Key and Override Register — Controlling Mechanical Fallback Access

Day 4: Alarm Response and Audit Trails

- Door-Forced and Door-Held Alarm Triage — Prioritising Control Room Response
- Alarm Response Playbooks — Defining Who Attends, Checks and Records
- Event Log and Audit Trail Reports — Answering Who Entered Where and When
- Periodic Access Recertification Cycle — Removing Rights Managers No Longer Approve
- System Health and Offline Reader Checks — Keeping Door Records Trustworthy

Day 5: Practising the Site Access Control Plan

- Zoning and Access Level Rebuild — Applying Day Two Templates to a Case Site
- Visitor and Contractor Scenario Run — Testing Day Three Rules Under Pressure
- Alarm Exercise and Log Review — Rehearsing Day Four Triage and Reporting
- Peer Challenge of Policy Exceptions — Defending Each Override Before Colleagues
- Site Access Control Plan Completion — Zones, Credentials, Alarms and Review Cycle

Applying Physical Access Control Systems After the Course

- Run a first access recertification on one high-risk zone and remove rights that managers no longer approve.
- Pull a door-held alarm report for the busiest entrance and agree a fix with facilities for the worst offending doors.

Physical Access Control Systems Questions FAQ

What are physical access control systems and why do they matter now?

Physical access control systems decide who may pass which door and when, and record every attempt. They matter now because contractor turnover and audit demands make unmanaged cards a visible liability.

Which roles gain most from physical access control systems training?

Security and facilities supervisors gain most. Each controls part of the entry chain, from issuing credentials to answering door alarms.

How does physical access control systems training differ from security screening training?

It concentrates on doors, credentials and records rather than searching people and bags. Screening courses cover checkpoint inspection; this one covers zoning, access rights, visitor entry and audit trails.

What do you bring back from physical access control systems training?

You bring back a site plan you can start using at once. It sets out zones, credential rules, visitor profiles, alarm triage and a recertification calendar.

Physical Access Control Systems: The Way Forward

The Site Access Control Plan first informs which doors move into a stricter zone and which credentials are withdrawn. Supervisors use it daily and site managers use it for audits. After the first recertification cycle, revisit the balance between strict anti-passback rules and the flow of people at peak shift changes.