

Red Cell Solutions

The 60-Point Physical Security Checklist

By Christopher Orta, Physical Security Consultant

Work from the outside in, the same direction an intruder would. Mark each item as you walk the facility. Every item you cannot confidently check off is a finding to record and prioritize. Full instructions: redcellsolutions.com/company/physical-security-checklist.html

Perimeter and Grounds

- ☐ Walk the full property boundary and confirm fencing, walls, and gates are intact and in good repair
- ☐ Check exterior lighting at night: parking areas, walkways, and every entrance, with no dark gaps
- ☐ Confirm landscaping is trimmed so it cannot conceal a person or block camera sightlines
- ☐ Verify signage marks restricted areas and directs visitors to the correct entrance
- ☐ Confirm dumpsters, ladders, and stored equipment cannot be used to reach the roof or upper windows
- ☐ Check that parking areas are visible from occupied spaces or covered by monitored cameras
- ☐ Note every route where someone could approach the building unobserved

Entry Points and Doors

- ☐ Test every exterior door: it should close and latch fully on its own, with no slipping or misalignment
- ☐ Look for propped or wedged doors, and ask whether staff understand why that matters
- ☐ Inspect door frames, hinges, and strike plates for resistance to prying and forced entry
- ☐ Confirm windows, roof hatches, loading docks, and utility entrances lock and are included in alarm coverage
- ☐ Verify emergency exits allow egress but do not permit re-entry from outside
- ☐ Give secondary and after-hours entrances the same scrutiny as the front door
- ☐ Check ground-floor windows for working locks and intact glazing

Access Control

- ☐ Confirm access is granted by role, with sensitive areas limited to the people who genuinely need entry
- ☐ Verify badges and keys are inventoried, and credentials are recovered or deactivated the day someone departs
- ☐ Confirm access logs exist and someone reviews them for anomalies on a regular schedule
- ☐ Check badge technology: legacy card formats can be cloned with inexpensive commercial tools
- ☐ Verify master keys are strictly limited, logged, and stored securely
- ☐ Confirm server rooms, records storage, and cash or pharmaceutical storage have their own access layer
- ☐ Watch a controlled door for ten minutes and count how many people tailgate through

Cameras and Surveillance

- ☐ Confirm cameras cover all entrances, receiving areas, and paths to critical assets, with no blind corners
- ☐ Pull sample footage and check both retention length and image quality
- ☐ Confirm someone is responsible for reviewing footage or responding to camera alerts, not just recording
- ☐ Re-verify camera positions after any renovation, furniture change, or landscaping growth
- ☐ Confirm recording equipment is physically secured so an intruder cannot remove the evidence
- ☐ Check whether cameras still produce usable images at night and in bad weather

Alarms and Detection

- ☐ Confirm intrusion detection covers every exterior entry point, not just the front and back doors
- ☐ Verify the alarm system has been tested recently and the test is documented
- ☐ Record the system's age: older panels and wireless sensors may use protocols that modern tools can defeat
- ☐ Confirm alarm response is defined: who is called, in what order, and how quickly
- ☐ Verify arming and disarming codes are individual, not shared, and are changed when staff leave
- ☐ Confirm duress or panic alarms exist where staff face the public alone, and staff know how to use them
- ☐ Ask when the last false alarm occurred and how it was handled

Visitor Management

- ☐ Confirm all visitors sign in, show identification, and receive a visible badge that expires
- ☐ Verify visitors are escorted in non-public areas, and contractors and vendors are verified before entry
- ☐ Confirm staff are trained to challenge or report anyone without a visible badge, regardless of appearance
- ☐ Verify tailgating through controlled doors is prohibited and the rule is actually enforced
- ☐ Confirm deliveries are received at a defined point and drivers do not roam the facility
- ☐ Review the visitor log for completeness over the past month

Personnel Practices

- ☐ Confirm new hires receive security orientation and all staff get recurring awareness training
- ☐ Verify background screening appropriate to the role is performed before granting access
- ☐ Confirm departing employees have access revoked, credentials collected, and codes changed promptly
- ☐ Ask staff how they would report suspicious behavior and whether they feel safe doing so
- ☐ Walk the office and check for credentials, keys, and sensitive papers left in the open
- ☐ Confirm social engineering awareness is trained: impersonation of IT staff, inspectors, and maintenance workers is a standard intrusion technique
- ☐ Test the challenge culture: would anyone stop an unfamiliar, unescorted person walking the halls

Documents and Sensitive Materials

- ☐ Confirm paper records with personal, medical, legal, or financial data are stored in locked rooms or cabinets
- ☐ Verify documents are shredded or destroyed under a defined retention and disposal policy, never just discarded
- ☐ Confirm server rooms and network closets are locked at all times and never used for general storage
- ☐ Verify laptops, backup media, and portable devices are secured when unattended
- ☐ Check printers, copiers, and fax areas for sensitive output left in the open
- ☐ Confirm whiteboards and displays visible from windows or public areas do not reveal sensitive information
- ☐ Check the dumpster: nothing sensitive should leave the building unshredded

Incident Response and Emergency Planning

- ☐ Confirm a written plan covers intrusion, theft, workplace violence, fire, and severe weather
- ☐ Verify every incident and near miss is reported, recorded, and reviewed for patterns
- ☐ Confirm roles are assigned: who calls law enforcement, who directs staff, who communicates afterward
- ☐ Verify evacuation and lockdown procedures have been practiced, not just written
- ☐ Confirm emergency contact lists are current and accessible without network or power
- ☐ Confirm findings from past incidents fed back into your security controls

Need help turning findings into a plan? Red Cell Solutions conducts physical security assessments, audits, and penetration tests. Call 954-496-0657 or email contact@redcellsolutions.com. More resources at redcellsolutions.com