Who belongs on a Level 1 facility access list?

Approved physical access: the core question

A Level 1 facility security program asks one practical question about every person who enters: does this individual need to be here, and are we certain of their identity and clearance? The approved physical access list is the document that answers that question before anyone reaches the door. It is not a phone directory of everyone who works in the building. It is a controlled register of people who have a justified need to enter a protected work area and who have passed the required identity verification and authorization checks.

The list should include only personnel whose roles directly depend on access to the area where controlled goods or information are handled. That typically means cleared employees, contractors with a valid security screening, and occasional visitors who are sponsored by a cleared employee and remain escorted. The key is that every entry has a reason attached to it, and that reason is reviewed periodically. A person who no longer needs access should be removed promptly, not left on the list indefinitely.

Who should definitely be on the list

Start with the people who work inside the protected area every day. Their names, their company affiliation, their clearance level, and the specific area they are authorized to enter should all be recorded. For a Canadian defence supplier working to CPCSC Level 1 requirements, the list also needs to show the date of the most recent identity verification and the name of the person who authorized the access. This is not about tracking every movement inside the building. It is about knowing, at any moment, who is permitted to be there at all.

Contractors and service technicians who need occasional access should also appear, but their entries are different. They should be listed with a start and end date for their authorization, and the list should note whether they require an escort. A cleaner who works after hours, for example, may have a standing authorization that is renewed annually. A visiting equipment repair technician might have a single-day entry that expires at the end of the shift.

One common gap is the treatment of sub-contractors. A prime contractor may have a cleared employee on site, but that employee may bring along a sub-contractor who has not been vetted. The approved access list should require that every individual, regardless of who they work for, is listed separately and has passed the same identity check. No exceptions for "he is with us" or "she comes with the delivery."

Who does not belong on the list

The list is not a badge for everyone who passes through the lobby. People who work in the same building but have no business in the protected area are not appropriate entries. A receptionist who works in the front office but never enters the secure zone does not need to be on the approved physical access list. Neither does a building maintenance person who only services common areas. If a person does not have a genuine, recurring need to be in the protected work area, they should not appear.

Visitors who are infrequent and escorted can be handled through a separate visitor log rather than the main access list. The visitor log records their name, company, time of entry and exit, the name of the escorting employee, and the purpose of the visit. This keeps the approved list clean and focused on regularly authorized individuals. An auditor or a government inspector, for instance, would be entered in the visitor log rather than added to the permanent list, unless they are conducting repeated, unescorted inspections.

How the list connects to door control and key control

The approved access list is not a standalone document. It feeds directly into door control and key control processes. Each person on the list should have a corresponding credential - a card, a key, or a code - that is issued only after their name has been added. When a person is removed from the list, their credential should be recovered or deactivated the same day. A gap between removal and deactivation is one of the most common findings in security audits.

For a Level 1 facility, door control typically means physical locks with a controlled key system, or electronic access that logs every entry. The access list tells the door control system who is allowed through. If the system uses a card reader, the list should be synchronized with the cardholder database. If the system uses a paper sign-in, the list is the roster of people who may sign themselves in without an escort.

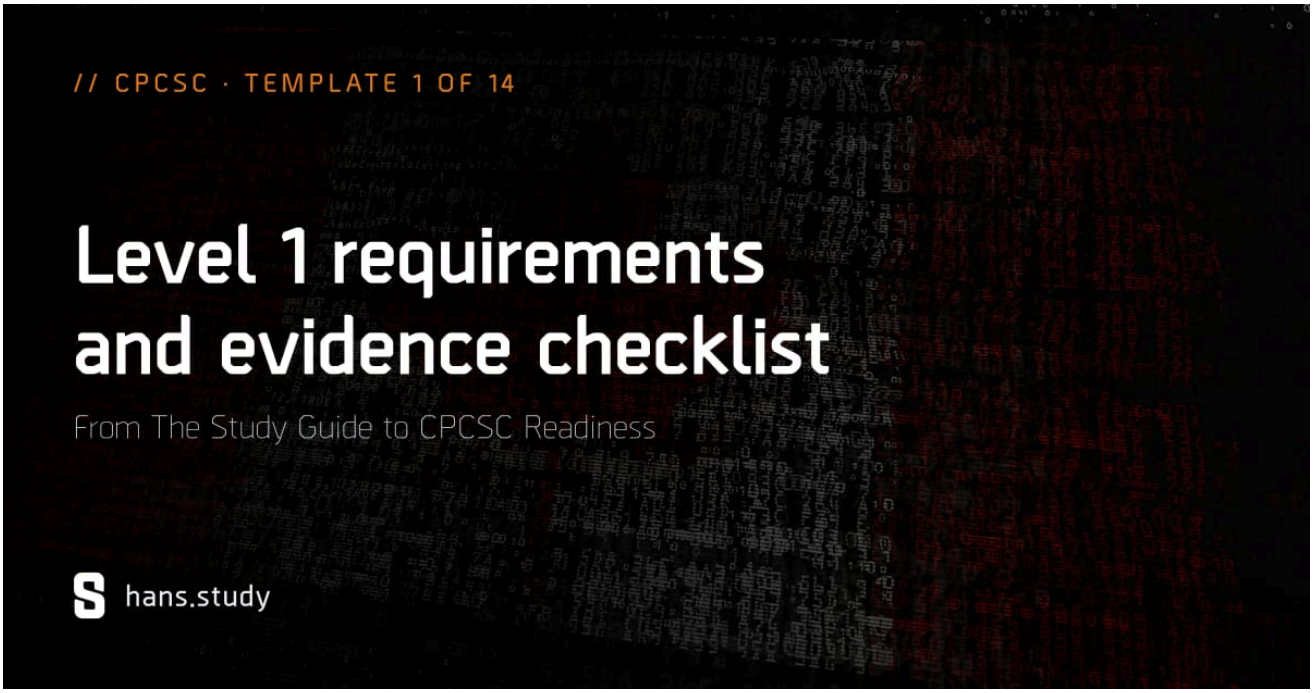
Key control is equally important. Every key or keycard that opens a protected area should be traceable to a named individual on the access list. Lost keys should trigger an immediate review of the list and, if necessary, a rekey of the affected area. The key control log and the approved access list should be cross-referenced regularly to ensure that no credential is outstanding for a person who is no longer authorized.

Access authorization and the role of evidence

Access authorization is the decision to add someone to the list. That decision should be made by a designated security officer or facility manager, not by a supervisor who happens to be nearby. The authorization should be recorded in writing, and it should reference the evidence that supported the decision. That evidence typically includes a valid government-issued photo

ID, a security clearance certificate or confirmation from the contracting authority, and a signed acknowledgment of the facility's security rules.

The phrase "evidence from the protected work area" describes exactly what the authorization should be based on. It means that the evidence used to approve someone must come from the area they will be entering - not from a scanned copy sent by email, not from a photo taken in the parking lot. The physical ID check should happen at the entrance to the protected area, by someone who is trained to verify identity documents. This is not about distrust. It is about making sure that the person standing at the door is the same person whose name appears on the clearance certificate.



When a person leaves the organization or no longer needs access, the same standard applies. The removal should be documented, and the evidence from the protected work area - in this case, the returned credential and the signed off-boarding checklist - should be filed with the access list. Keeping a clean chain of authorization is part of what makes the list defensible during an audit.

Sanitization records, destruction logs, and retired media

An often overlooked part of physical access management is what happens to records and materials that leave the area. If a person on the access list handles classified or controlled information, their departure should trigger a review of sanitization records and destruction logs. Any retired media that was used by that individual should be accounted for. This is not directly about the access list itself, but it is a natural extension: the list tells you who had access, and the sanitization and destruction logs tell you what they left behind.

For a defence supplier, the connection between the access list and these logs is important for compliance. An auditor will look at whether the facility can demonstrate that, when a cleared person left, their access was terminated and any materials they controlled were properly handled. The approved physical access list is the starting point for that demonstration.

Practical tips for maintaining the list

Keep the list in a format that can be updated quickly but not tampered with. A spreadsheet that anyone can edit is too loose. A printed PDF that is updated weekly and signed by the security officer is better. An electronic database with an audit trail is best for a larger facility. Whatever format you choose, the list should include at minimum: full legal name, company or organization, clearance level and expiry date, area authorized, date of last identity verification, and the name of the authorizing official.

Review the list at least quarterly. Look for names that have not badged in during the review period. Check that every person still has a current clearance. Remove anyone who has left the project or whose clearance has expired. A stale list is worse than no list, because it gives a false sense of control.

Train the people who manage the list. They should understand that adding a name is not a formality. It is a security decision that carries the same weight as locking a door. They should also know how to handle a situation where someone refuses to present the required evidence. The answer is simple: that person does not get on the list.

The phrase "evidence from the protected work area" appears in this discussion because it captures the principle that verification must happen at the point of access, not in a back office. A manager who approves an access request from a desk without seeing the person's ID is creating a gap. The list is only as trustworthy as the evidence behind each entry.

Keeping the list practical

An approved physical access list does not have to be complicated. For a small facility with a handful of cleared staff, a paper log that is updated after every change may be perfectly adequate. For a larger site with multiple work areas and shift workers, an electronic system that integrates with the door control system is better. The important thing is that the list exists, that it is accurate, and that it is used as the basis for every access decision.

Remember that the list is a tool, not a wall. It works best when it is complemented by a visitor log, a key control register, and a clear policy for reporting lost credentials. The goal is not to make entry difficult. It is to make unauthorized entry impossible, and to prove in an audit that every authorized entry was justified.