

Camera access tends to grow quietly. A facilities manager gets a login, a contractor is given temporary access, and a former employee's account stays active because nobody owns the offboarding step. Months later, the access list no longer reflects who actually needs to view or export footage.

A sensible starting point is to **audit user accounts at least quarterly**, with additional checks whenever someone joins, changes role, leaves, or a supplier's work ends. The right **permission review cadence** depends on the number of cameras, the sensitivity of the areas covered, and how many people can view or export recordings. The aim is not to review footage more often. It is to make sure each person's access remains necessary, limited and accountable.

Before adding or retaining any access, ask: **"What security question does this camera answer?"** If there is no clear answer, revisit whether the camera or the access is needed at all.

Start with a clear access-review schedule

There is no single review interval that suits every building. A small residential block with a single authorised operator may need a lighter process than a mixed-use site with a concierge team, security contractor and multiple managers. As a practical baseline, use this schedule and adjust it to the risks and responsibilities in your building:

When	What to review	Who should take part	At least quarterly	Active accounts, roles, permissions, recent exports and temporary access
		System owner and authorised site or property manager	When someone leaves or changes role	Disable or amend access promptly; check shared credentials and linked supplier accounts
		Line manager, HR or contract owner, and system administrator	At supplier or contract change	End old accounts, confirm data return or deletion, and approve any replacement access
		Contract owner and system owner	After an incident, complaint or system change	Review who accessed relevant footage, why, and whether permissions or procedures need changing
		Incident lead and appropriate governance contact		

Quarterly is a useful default, not a substitute for event-driven action. Do not wait for the next scheduled audit to **remove former employees** or revoke a contractor's access after their duties end. If your system supports automatic account expiry, use it for temporary access rather than relying on someone to remember later.

What does a proper account audit include?

A list of usernames is not enough. For each account, record who uses it, what they can do, why they need that access, who approved it and when it should be reviewed. Make the review easy to evidence: a dated log or approved checklist is more useful than an informal "we checked it" message.

During each review, check:

- **Identity:** Does the account belong to a named individual? Avoid generic logins such as "night staff" where the system can support individual accounts.
- **Purpose:** Is there a current, documented work reason for access?
- **Scope:** Can the person see only the cameras and functions required for their role?
- **Actions:** Can they view live feeds, search recordings, export clips, change settings, or create accounts? These are different levels of access.
- **Status:** Has the person left, changed role, or finished their contract?
- **Authentication:** Are strong passwords and multi-factor authentication available and enabled, particularly for remote access?

- **Activity:** Are access and export logs available, and have unusual or unexplained actions been followed up?

Where possible, apply role-based permissions. For example, a staff member who checks a live entrance feed may not need the ability to export recordings or administer the whole system. Keep administrator rights to a small number of people, and use separate named accounts rather than sharing one powerful login.

Give ownership and governance a named home

Access reviews fail when everyone assumes someone else is responsible. The building owner, management company, HOA or residents' association may have a role in deciding why surveillance is used, while the property manager or security provider may operate the equipment. Write down who makes decisions, who carries them out, and who handles requests or complaints.



A straightforward governance record should identify:

- the organisation or person responsible for the surveillance decisions;
- the system owner who approves accounts and permissions;
- the operational administrator who manages users and settings;
- the person responsible for checking access logs and recording review outcomes;
- the process for approving footage exports and responding to requests; and
- the contact who reviews the arrangement with the board, committee or relevant management group.

In the UK, organisations using CCTV should consider their data protection responsibilities, including the UK GDPR and Data Protection Act 2018, and consult current Information Commissioner's Office guidance. The appropriate arrangements depend on who decides the purposes and means of processing. A management agreement or supplier contract does not, by itself, remove the need to understand who is responsible for decisions.

Keep governance proportionate. A board does not usually need to watch routine footage to oversee the system. It should receive enough information to check that the purpose, access controls, retention and complaints process remain appropriate—without turning camera monitoring into an activity in its own right.

Limit access by limiting what the cameras can see

Permissions are only one part of data minimisation. The camera's placement and field of view determine what footage is collected in the first place. A well-controlled account can still expose more personal information than necessary if a camera captures homes, neighbouring land, staff areas or unrelated public space.

Review camera positioning when the system is installed, after building works, when the use of an area changes, and as part of a periodic site review. For each camera, record its purpose, location, field of view and who has access. Check whether the lens can be adjusted, privacy masking applied, or a feature switched off when it is not needed.

For example, a camera intended to help investigate unauthorised entry may not need to capture a whole reception area or a resident's front door. A garage camera may need to cover vehicle access points without recording more of a neighbouring property than necessary. Test the actual view on screen; do not rely solely on a floor plan or installer's description.

Access should follow the same principle: give each person only the camera views and system functions needed for their duties. Ask, "What security question does this camera answer?" and "Does this user need to see this view to answer it?" If either answer is unclear, pause and review the purpose and permissions.

Control exports and keep a record

Viewing footage and exporting a clip are not the same risk. An export creates another copy that can be stored, shared, or forgotten outside the camera platform. Restrict export permissions and use an approval process that records the reason, date, person authorising it, footage range and recipient.

Always ask where exported clips end up and who can open them. Use an approved, access-controlled destination rather than personal email, messaging apps or an unmanaged shared folder. Set a deletion date when the clip is created, and confirm what happens to copies held by a supplier or another recipient. Do not circulate raw clips casually; disclose only what is necessary for the stated purpose, and consider appropriate redaction.

A redaction checklist should go beyond faces and vehicle registration plates. Depending on the footage, check for:

- children, visitors and bystanders who are not relevant to the incident;
- door numbers, access codes, keypads or other security details;
- computer screens, paperwork, package labels and personal correspondence;
- audio or speech, if the system captures sound;
- reflections or background views that reveal people or areas outside the intended scene; and
- metadata or accompanying notes that identify people unnecessarily.

Keep an export log. It should show who requested and approved the clip, who prepared it, where it was stored, who received it, the purpose, any redactions and the planned deletion date. If the request relates to a complaint, incident or legal matter, follow the organisation's established process and seek appropriate advice where needed.

Make retention and routine deletion part of the review

Access controls cannot fix a retention period that is longer than necessary. Set a documented retention period based on the surveillance purpose and operational need, rather than keeping everything indefinitely "just in case". Most routine footage should be deleted automatically when the period expires, unless a specific clip needs to be preserved for a documented reason.

During the quarterly review, check that automatic deletion is working, the period remains justified, and any retained incident clips have an owner and review date. Confirm that copies exported to other locations are covered by their own deletion arrangements. A shared folder with no deletion date is not a retention policy.

If footage is preserved for a complaint or investigation, record why, who authorised it, where it is held, who can access it and when the need will be reviewed. Once the reason ends, securely delete it according to the organisation's process. Avoid changing the retention period across the whole system just to preserve one clip; where possible, isolate the relevant footage.

How to run the review without making it a paperwork exercise

1. **Export the current user list.** Include roles, permission levels, account status and last-login information where available.
2. **Compare it with current staffing and contracts.** Confirm each named user with their manager or contract owner.
3. **Check permissions against duties.** Reduce access where someone can view or export more than their role requires.
4. **Remove former employees.** Disable accounts promptly and check for shared passwords, remote access and supplier accounts.
5. **Review camera views and purpose.** Confirm that each camera still has a defined security purpose and captures no more than needed.
6. **Check exports and retention.** Sample the export log, verify storage and recipients, and confirm deletion dates.
7. **Record decisions and actions.** Note the reviewer, date, exceptions, approvals and completion date for follow-up items.

If your system cannot provide individual accounts, activity logs or reliable expiry controls, record that limitation and agree a proportionate improvement plan. Do not treat a technical limitation as a reason to leave access

unreviewed. In the meantime, tightly control credentials, document who has them, change them when access needs change, and consider whether the system is suitable for the building's needs.

Common mistakes to avoid

- **Reviewing only after an incident:** Regular reviews catch stale access before a complaint or breach.
- **Keeping accounts “just in case”:** Access should have a current purpose, not a vague future possibility.
- **Using one shared account:** It makes it difficult to establish who viewed or exported footage.
- **Assuming the supplier owns the decision:** Clarify who sets the purpose, approves access and oversees the service.
- **Keeping broad views or permissions by default:** Limit both what the camera captures and what each user can see.
- **Leaving exports in unmanaged storage:** Record where clips go, who can open them and when they must be deleted.

What about prices?

No prices are listed here, because the cost of a camera system or access-control service depends on the equipment, site, number of users, support arrangements and any required upgrades. Do not assume that a particular review cadence has a standard price. Ask suppliers for an itemised quotation that separates installation, licensing, support, storage, training and any fees for account management or audit reporting. Compare what is included, and confirm that your organisation retains clear control over user access, footage exports and deletion.

A practical rule to take away

For most buildings, make a quarterly **permission review cadence** the routine baseline, and act immediately when a person's role or contract ends. Keep a named owner, use individual accounts, limit permissions and camera views, log exports, and routinely delete footage when its retention period expires. The point is not simply to count users. It is to be able to explain why each person has access, what they can see, and when that <https://realtytimes.com/new-headlines/cctv-in-elevators-and-common-areas-property-manager-responsibilities> access will be checked again.

Share this article

- Share on Facebook
- Share on X (Twitter)