

“We might need it one day” sounds like a sensible reason to keep security footage. In practice, it can turn a useful camera system into a growing store of sensitive information that nobody has a clear reason to retain. Footage of residents, visitors, staff, <https://realtytimes.com/new-headlines/cctv-in-elevators-and-common-areas-property-manager-responsibilities-deliveries-and-passers-by> may reveal where people live, when they come and go, who visits them and what they do in shared spaces.

For a building, the better question is not simply how much storage is available. It is: **what security question does this camera answer, and how long is the footage genuinely needed to answer it?** A clear purpose, controlled camera views and routine deletion are more reliable safeguards than keeping everything indefinitely.

This guide explains the risks of indefinite retention, how to set a practical **retention policy for a building**, and how to govern CCTV decisions in a way that supports security without collecting more than necessary. It is general operational guidance, not legal advice; check the rules that apply in your location and seek advice where needed.

What does “indefinite retention” mean?

Indefinite retention does not always mean someone has deliberately decided to store footage forever. It often happens by default: the recorder is set to retain as much as its hard drive allows, old clips are not overwritten, or exported files are copied into folders with no deletion date.

That default can be easy to overlook. A system may appear to have a short recording cycle, while incident clips, backups or downloads remain elsewhere. A complete retention review should therefore cover the entire footage lifecycle—not only the settings on the recording device.

The risks of keeping CCTV footage forever

More footage means greater privacy exposure

Security video can disclose patterns of movement and personal routines, even when nobody is suspected of wrongdoing. A long archive makes it easier to search for those patterns over time. That creates **privacy exposure from security video** that grows as the archive grows.

Data minimisation is the practical alternative: collect only what is needed for a defined security purpose, limit who can access it and delete it when that purpose no longer justifies keeping it. In a residential building, this may mean checking whether a camera needs to cover an entire lobby, or whether a narrower view of an entrance is sufficient.

A larger archive is a larger security target

Footage can be exposed through compromised accounts, poorly secured devices, misdirected emails, shared links or unauthorised access by people with legitimate credentials. The more video that is retained, the more material may be affected by a single incident.

Keeping old clips also creates a practical question that is often missed: **where do exported clips end up, and who can open them?** A clip downloaded for an incident may be copied to a personal laptop, attached to an email or placed in a shared folder. Each copy is another place to secure, track and eventually delete.

Old footage invites access without a current purpose

When a clip is kept “just in case”, staff may later view it out of curiosity or use it to answer questions unrelated to the camera’s original purpose. Access controls and staff training matter, but a shorter, justified retention period also reduces the opportunity for casual viewing.

In my experience reviewing building incidents, it helps to ask: **who needs this footage to do their job, and for what specific task?** “Because they can access the recorder” is not a good answer.

More data creates more work and uncertainty

Long-term footage brings administrative burdens: locating relevant clips, checking access history, responding to requests, managing exports and confirming that copies have been deleted. It can also make it harder to give a clear, consistent explanation to residents, staff or an oversight body about what is held and why.

Start with purpose, not the camera

Before installing a camera—or changing its view—write down the security problem it is intended to address. Be specific. “Improve safety” is broad; “record the main vehicle entrance so the team can investigate reported unauthorised access” is more useful.

Use these questions to test whether a camera is justified:

- What incident or risk is the camera intended to help address?
- Is CCTV necessary, or could lighting, access control, a patrol or a design change work?
- What is the minimum area that needs to be in view?
- Who will review footage, and under what circumstances?
- What is the shortest reasonable period for routine retention?

“We might need it someday” is not a camera purpose. Nor is adding cameras simply because equipment is available. Every camera should have a documented reason that can be reviewed when the building’s needs change.

Camera placement and field of view are part of data minimisation

Retention is only one part of a proportionate CCTV setup. A camera that unnecessarily captures private areas or broad stretches of public space collects more information than the building may need, even if footage is deleted promptly.

Design the view deliberately

During installation and periodic reviews, check what the camera actually records at different times of day and in different lighting. Consider whether the image includes windows, neighbouring property, private doorways, desks, seating areas or places where people reasonably expect greater privacy. Adjust the angle, zoom or masking features where appropriate.

For each camera, keep a simple record of its location, purpose, field of view, responsible owner and review date. If the environment changes—such as a renovation, new entrance or changed pedestrian route—reassess the view rather than assuming the old setup is still suitable.

Who owns CCTV decisions in a building?

Camera decisions should have an accountable owner. In a mixed-use or managed building, responsibilities may involve the owners' association or board, property manager, onsite team, security contractor and technology provider. If ownership is vague, important tasks—such as approving access, setting retention and checking exports—can fall between roles.

Agree who is responsible for:

- approving camera purposes, locations and changes;
- maintaining the system and configuring routine deletion;
- authorising and recording access to footage;
- handling incident-related exports and requests;
- checking that copies are stored securely and deleted on time; and
- reviewing the policy and training relevant staff or contractors.

Governance should also identify who can approve an exception to the normal deletion schedule, what evidence or reason is required, and when that exception will be reviewed. A contractor may operate the equipment, but that does not remove the need for the building's responsible decision-makers to understand and oversee the arrangement.



Set a retention period that fits the purpose

There is no single number that suits every building. A sensible period depends on the camera's purpose, the time it may take for an incident to be reported, system capacity and applicable legal requirements. The key is to choose a defined period, document why it is appropriate and review it—not leave the system on an open-ended setting.

Footage type Operational approach Control to document Routine recordings Overwrite or delete automatically after the approved period. Retention setting, owner and review date. Incident clip Keep only when there is a defined, ongoing reason to preserve it. Incident reference, authorised access and review or deletion date. Exported copy Store in an approved, access-controlled location—not in general email or open shared folders. Named custodian, permitted users and deletion confirmation.

The table is a planning aid, not a universal legal schedule. Building management should set actual periods based on the purpose and applicable requirements, then make sure the system can enforce them.

Make routine deletion real

A policy is only useful if it matches what happens in practice. Configure automatic overwriting or deletion where possible, and test that the setting works. Include backups, exports and copies made for investigations; otherwise routine footage may disappear while retained copies quietly accumulate.

For footage preserved because of a specific incident, record why it is being held, where it is stored, who can access it and the date it must be reviewed. At review, confirm whether the reason still applies. When it does not, delete the clip and document the action.

Keep an access and disclosure log for meaningful viewing, export or sharing events. A basic entry should identify the date, person, footage or incident reference, reason, authorisation and any recipient. Avoid emailing raw clips around as a convenient shortcut. Use an approved secure method, share only what is necessary and record where the copy went.



Common mistakes to avoid

- **“The hard drive has room, so keep more.”** Storage capacity is not a purpose or retention justification.
- **Leaving cameras running “just in case”.** Reassess cameras that lack a specific, current security question.
- **Assuming deletion happens everywhere.** Check exports, backups, contractor systems and shared folders.
- **Allowing casual viewing.** Limit access to people with a work-related need and explain the rules.
- **Creating shared-folder dumps with no deletion date.** Give every retained copy an owner, access limit and review or deletion date.

Do not rely on unverified prices or copied claims

Some scraped articles include no prices, or repeat figures without explaining what they cover. Do not fill that gap with invented CCTV costs or copy a number from an unrelated source. Equipment, storage, installation, maintenance and secure export arrangements vary by building and supplier. If a board needs a budget, request comparable quotes and identify exactly what each includes.

Likewise, avoid treating a copied retention period as a universal rule. The right schedule depends on the building's purpose and the requirements that apply. Document the reasoning and seek qualified advice where the situation calls for it.

A practical review checklist

1. List every camera and state the specific security purpose it serves.
2. Review each field of view and reduce unnecessary capture.
3. Name the people accountable for system settings, access and exports.
4. Set and document a defined routine retention period.
5. Test automatic deletion and check for retained copies outside the recorder.
6. Log authorised access, disclosure and incident-related preservation.
7. Assign a deletion or review date to every exported clip.
8. Revisit the policy and camera layout when building conditions or risks change.

Keep what you need, delete what you do not

CCTV can support building security, but an unlimited archive is not automatically a safer one. Indefinite retention increases privacy exposure, expands the consequences of a security breach and makes oversight harder. A proportionate approach starts with a clear purpose, limits the camera's view, assigns ownership and makes routine deletion part of normal operations.

Before approving a new camera or a longer retention period, ask the reality-check question: **what security question does this footage answer?** Then ask where any exported clips will end up, who can open them and when they will be deleted. If those answers are unclear, the system needs better governance—not a bigger archive.

Share this article

- [Share on Facebook](#)
- [Share on X \(Twitter\)](#)