Security cameras can help property teams investigate incidents, protect shared spaces and understand what happened when accounts differ. But more cameras do not automatically mean more security. Poorly planned systems can capture more personal information than necessary, create avoidable disputes and leave sensitive footage accessible to too many people.

Before installing a camera or exporting a clip, ask a quick reality-check question: **What security question does this camera answer?** If there is no clear answer, the camera may be recording people without a sufficiently defined purpose. The same discipline should apply to camera angles, access permissions, retention periods and decisions about sharing footage.

Here are common mistakes property managers make with CCTV in residential and mixed-use buildings, and practical ways to avoid them.

1. Installing cameras “just in case”

Ever notice how a camera installed without a specific purpose tends to become a general-purpose recording device. That can mean continuous monitoring of residents, visitors, staff and contractors without a clear reason for collecting the footage. It can also create expectations that the camera will prevent or resolve every incident.

Start with a documented security need. For example, a camera may be intended to help investigate unauthorised access to a garage entrance or repeated damage to a mailroom. Identify the incident or risk, the location where it occurs, and how footage could reasonably assist. Consider whether less intrusive measures—such as improved lighting, a controlled-access door or a concierge procedure—could address the problem.

Data minimisation is a useful test throughout this process: collect only what is necessary for the stated purpose. If a camera would capture a whole courtyard to monitor one door, see whether a narrower view can do the job. If an access-control log or a targeted patrol is sufficient, recording everyone in the area may be excessive.

2. Leaving ownership and governance unclear

“The building has cameras” is not a governance plan. In a shared building, it may be unclear whether the owners’ corporation, management company, landlord or another party decides what the system records and who can review it. That uncertainty becomes a problem when a resident requests footage, a board member wants access or an incident requires prompt preservation.

Set out who is responsible for the system and who has authority to make decisions. The arrangement will depend on the building and applicable law, but a written policy should normally cover:

- the purpose and locations of each camera;
- who approves installation, relocation or changes to the field of view;
- who can view live images and recorded footage, and for what reasons;
- how access and exports are logged;
- how requests, complaints and disclosure decisions are handled; and
- who reviews the policy, system and supplier access.

Make a simple camera register and keep it current. For each device, record its location, purpose, general field of view, recording settings, retention period and responsible decision-maker. That helps a manager explain why a camera exists and spot equipment that has been left in place after its original purpose has changed.

3. Using overly broad camera views

Overly broad camera views are among the easiest mistakes to miss. A camera aimed at a shared entrance may also capture a neighbouring home's windows, a private patio, a staff break area or more of a footpath than the building needs to monitor. A wide-angle lens can make this happen even when the camera looks as though it is pointed at one doorway.

Test the actual recorded image, not just the camera's position. Check it at different times of day, with lighting changes and after any adjustment to the lens or mounting. Ask whether the camera can be angled, zoomed or digitally masked so it records the relevant entrance without unnecessarily capturing surrounding areas. Review the image after maintenance or a camera replacement; a small change in mounting height can significantly alter the field of view.

Also consider whether recording is needed continuously. Where appropriate, motion-based recording or a narrower schedule may reduce unnecessary collection, though these settings should be tested to make sure they do not miss the events the system is intended to capture.

Check the view before signing it off

Use a short site checklist rather than relying on a contractor's description of the camera. Confirm what can be seen in the live view and in a saved recording, whether masking is active, and whether the system can be configured to avoid capturing areas outside the building's legitimate security need. Document the agreed view so later changes can be identified.

4. Assuming a camera is harmless because it is in a common area

A lobby, lift or garage may be a shared space, but that does not make unlimited monitoring appropriate. People can still have reasonable expectations about how their movements are recorded and who can inspect the

realtytimes.com footage. A camera inside a lift, for example, may capture passengers at close range throughout their journey; a camera outside an apartment door may reveal patterns of visits.

Assess each location on its own merits. Consider how sensitive the space is, how many people pass through it, whether the camera captures identifiable details and whether a less intrusive option would work. Be especially careful about areas where people may expect greater privacy, including changing facilities, toilets and private residential spaces. Do not assume that placing a notice nearby resolves every concern.

Clear notices matter, but they are only one part of responsible surveillance. They should help people understand that cameras are operating, who is responsible for them and how to make an enquiry. A notice cannot compensate for an excessive field of view or an unclear purpose.

5. Keeping footage indefinitely

Keeping footage indefinitely is not a sensible default. It increases the amount of sensitive information held and the potential harm if an account is compromised, a system is misused or a clip is disclosed incorrectly. It can also make incident reviews harder: staff may not know which recordings are still relevant or whether older footage should have been deleted.

Set a routine retention period based on the purpose, the system's capabilities and applicable legal requirements. The period should be long enough to allow a relevant incident to be reported and reviewed, but not simply "as long as the recorder has space". Record the period in the policy and configure the system to overwrite or delete footage automatically where possible.

If a particular clip needs to be preserved for an investigation, complaint, insurance matter or legal process, isolate that clip rather than extending retention for the entire system. Document why it was retained, who authorised the decision, who can access it and when its continued retention will be reviewed. When the reason ends, arrange deletion securely and record that action.

Situation Practical control Routine recordings Use a defined retention period and automatic deletion or overwrite. Relevant incident clip Preserve only the necessary segment, with a recorded reason and review date. Expired footage Delete it securely and keep an appropriate record of the deletion process.

6. Emailing raw clips

Emailing raw clips is convenient, but it can spread footage beyond the people who need it. An attachment may be forwarded, downloaded to a personal device or left in an inbox long after the incident has been resolved. It may also contain images of people unrelated to the matter, private information visible in the background or audio that was not intended to be shared.

Before exporting footage, confirm the purpose, authority and recipient. Share the smallest relevant segment and use a controlled, secure method with access limited to named people. Avoid sending raw clips through ordinary email or dropping them into a shared folder that has broad permissions and no deletion date.

Always ask: **Where will the exported clip end up, and who can open it?** Keep a disclosure log showing the date, requester, reason, footage supplied, recipient, approving person and method of transfer. Include any restrictions or expiry date for access. A log makes it possible to explain later what was shared and why.

Redaction checks go beyond faces and number plates

Redaction may be needed before footage is disclosed. Check not only faces and vehicle registration plates but also:

- screens, notices or documents visible in the image;
- apartment numbers, access codes or other security details;
- people in the background who are not relevant to the request;
- reflections that reveal people or spaces outside the main view; and
- audio or metadata that could identify someone or disclose unrelated information.

Do not assume a blurred preview means the exported file is redacted. Check the final copy, including the full duration and any audio, before sharing it.

7. Allowing casual or excessive access

People should not browse CCTV because they are curious, happen to be on site or know how to use the monitoring software. Broad access increases the risk of inappropriate viewing, accidental disclosure and inconsistent decisions. It can also undermine trust in the management team.

Use role-based permissions: give each person only the access they need for their duties. Separate the ability to view live images from the ability to export or delete recordings where the system allows it. Use individual accounts rather than shared logins, review permissions when staff or contractors change roles, and keep an access log. Train authorised users to view footage only for a defined operational purpose and to raise requests through the agreed process.

8. Buying or describing a system without clear costs

Another common mistake is leaving costs unclear during procurement. If a supplier page, scraped article or project summary has **no prices listed**, do not treat that as a price or imply that a system has a particular cost. CCTV expenses can depend on the number and type of cameras, cabling, installation, storage, software, monitoring, maintenance and future upgrades.

Ask suppliers for an itemised quotation and clarify ongoing charges, contract length, data storage arrangements, support and who can access recordings. Compare proposals against the documented security need rather than choosing the largest system or the lowest headline figure. If you publish guidance for residents or a board, state plainly when prices are unavailable and explain how to request a current quotation. Do not invent or infer prices from an incomplete article.

9. Treating installation as the end of the job

A camera policy can become inaccurate as building layouts, risks and staff responsibilities change. A renovation may alter the view; a new entrance may make an old camera unnecessary; a supplier may change how footage is stored. Schedule periodic reviews, and review sooner after a significant incident, system change or complaint.

1. Confirm each camera still has a defined, necessary purpose.
2. Check field of view, privacy masking and recording settings.
3. Verify retention and automatic deletion settings.
4. Review user permissions, access logs and supplier access.
5. Check that export, disclosure and deletion procedures are followed.
6. Update the camera register and explain material changes to the appropriate stakeholders.

Make surveillance proportionate and accountable

Good camera management is not about recording as much as possible. It is about being able to explain what each camera is for, why its view is necessary, who governs its use and when recordings are deleted. Narrow fields of view, defined retention, limited access and careful exports reduce unnecessary exposure while keeping footage useful when a genuine incident occurs.

For every proposed camera or request for footage, return to two questions: **What security question does this camera answer?** And, if a clip is being shared, **where will it end up and who can open it?** Clear answers are a practical starting point for safer, more accountable building operations.

Share this article

- Facebook share
- X (Twitter) share