

CCTV EVIDENCE READINESS

YOUR CCTV CAPTURED IT CAN THE FOOTAGE PROVE ANYTHING?

A practical evidence readiness guide
for South African SMEs



energise business solutions
INNOVATE. CONNECT. ENERGISE

A camera can record an incident and still leave the business without useful evidence. This report explains how to test image quality, timestamps, retention, export, playback, access and handling before the day the footage is urgently needed.

SEPTEMBER 2026 • EDUCATIONAL BUSINESS TECHNOLOGY REPORT

EXECUTIVE SUMMARY

Executive Summary

The real test of a CCTV system is not whether pictures appear on a monitor. It is whether the business can find the correct incident, understand what the images show, export the relevant material promptly and explain how the file was handled.

The central management message: recording is only the first step. Useful evidence depends on image quality, correct time, sufficient retention, controlled access, reliable export and a documented handover.

A business may discover too late that the camera was aimed correctly but recorded too little detail; that the recorder clock was wrong; that the required footage was overwritten; or that the exported file will play only in unfamiliar proprietary software.

This report recommends a short monthly evidence readiness test. The test does not promise that footage will be accepted or given decisive weight in a legal process. It helps the business preserve reliability, context and a clear record of what happened to the footage.

Management should be able to answer five questions:

1. Can we retrieve a known event without calling the installer?
2. Can an ordinary authorised recipient open the exported file?
3. Are the date, time and camera identity reliable and understandable?
4. Can we show who exported, copied, viewed and handed over the footage?
5. Is our retention and access practice justified, documented and POPIA-aware?

MAIN ARTICLE

Your CCTV Captured the Incident

Why a recording can exist without becoming useful evidence

At 08:10 on Monday, the manager of a small distribution business discovers that stock disappeared from the loading area over the weekend. The cameras are online. The live view is clear. Yet the incident response quickly becomes a search through several days of recordings, uncertain clocks and camera names such as CAM03 and CAM07.

When the relevant clip is finally found, the person occupies only a small part of the frame. The export creates a file that will not open on a normal computer. Meanwhile, the recorder is continuing to overwrite old footage. The system recorded something, but the business was not ready to use it.

1 What makes footage useful

Useful CCTV evidence is a combination of content and process. The image must show enough relevant detail. The system must preserve the right period. The business must be able to retrieve and play the material. The date, time, camera and location must make sense. Access and copying must be controlled and recorded.

This is why a high-resolution specification alone is not enough. A wide camera view can look sharp while a face, registration plate or hand movement remains too small, blurred or badly lit to answer the question that matters.

2 Start with the incident question

Different cameras serve different purposes. An overview camera may show that a person entered an area. An identification view may be needed to recognise the person. A dedicated vehicle view may be needed to read a registration plate. Expecting one camera to do all three jobs can create false confidence.

A better requirement is specific: “Show which person removed cartons from the dispatch cage, the route used and the time of departure.” The scene, camera position, lighting and retention can then be tested against that requirement.

3 The eight points where evidence readiness fails

Failure point	What goes wrong	Monthly test
Coverage	The incident occurs outside the useful field of view or behind an obstruction.	Walk the likely route and review recorded—not only live—video.
Detail	The subject is visible but too small, blurred or overexposed to identify.	Test representative people, vehicles and movements by day and night.
Time	Recorder and camera clocks differ or drift.	Compare displayed time with a reliable reference and record the result.
Retention	The clip has been overwritten before anyone requests it.	Confirm actual retained days under normal and peak recording conditions.
Retrieval	Only the installer knows how to find an event.	Train at least two authorised staff members and test them.
Export	The file is proprietary, incomplete or loses context.	Export a native copy plus a commonly playable viewing copy where available.

Failure point	What goes wrong	Monthly test
Access	Shared passwords or broad app access leave no accountability.	Use named accounts, least privilege and review access logs where supported.
Handling	Copies circulate with no record of who created or received them.	Use an incident export record and preserve the first export unchanged.

4 Time is part of the evidence

An incorrect timestamp does not automatically make footage worthless, but it creates an avoidable question. The business may need to explain the size and cause of the difference and correlate the recording with access-control, alarm, till, phone or vehicle records.

Use a reliable time source and check whether cameras and recorders are synchronised. Record the time-zone setting and daylight-saving configuration; South Africa does not use daylight saving, but imported defaults may still be wrong. After a power failure, firmware update or equipment replacement, test again.

5 Retention should follow purpose and risk

There is no universal POPIA rule requiring every business to keep CCTV for a fixed number of days. Retention should be linked to a lawful and documented purpose, the time normally needed to discover an incident, contractual or legal requirements, storage capacity and the privacy risk of keeping identifiable footage longer than necessary.

The number shown in the recorder settings is not proof of actual retention. Motion levels, frame rate, resolution, compression, the number of cameras and failed storage can change the number of days available. Test the oldest footage that can actually be retrieved.

6 Export for use outside the recorder

An export is useful only if the intended recipient can open it and understand it. Some systems create proprietary files that require a player, codec or administrator rights. Others export a familiar video format but omit metadata or make it difficult to establish the camera, date or sequence.

Where the system permits it, preserve the native export and create a clearly labelled viewing copy. Include the vendor player or verified access instructions when required. Do not edit, enhance or transcode the preserved first export. If a working copy is prepared, label it as a derivative and keep a record of the steps performed.

Interoperability matters. ONVIF originally stood for Open Network Video Interface Forum. It is an industry forum that develops common standards to help IP-based security products from different manufacturers work together. Its export specification was designed to improve consistent sharing and playback, including timestamps and export metadata. Compatibility must still be confirmed for the exact camera, recorder, software version and export path being used.

7 Authenticity and chain of handling

South Africa's Electronic Communications and Transactions Act does not allow a data message to be rejected merely because it is electronic. When evidential weight is assessed, the reliability of generation and storage, the maintenance of integrity and the identification of the originator are relevant factors. Court decisions also show that relevance and authenticity can be disputed.

A simple handling record cannot decide admissibility, but it helps the business explain the footage. Record who made the export, when it was made, the system and camera used, the requested time range, the destination media, the recipients and every later copy. Preserve the original exported files and any accompanying player or metadata.

8 POPIA applies before and after an incident

CCTV footage can be personal information when it relates to identifiable people. Recording, storing, viewing, copying, sharing and deleting are all forms of processing. The responsible party should define the purpose of surveillance, limit access, use reasonable security safeguards, set and apply a retention approach and manage requests or disclosures through authorised people.

Footage should not be shared casually through personal messaging accounts or broad staff groups. When police, insurers, attorneys, employees or members of the public request footage, the business should follow a documented process and obtain advice where the circumstances are sensitive or disputed.

9 Who should own the process

The installer can configure equipment and assist with faults, but evidence readiness remains a management responsibility. The business should name an operational owner, an alternate and the person authorised to approve external disclosure. The Information Officer should be involved in the privacy and access rules.

PRACTICAL TOOL

Monthly CCTV Evidence Readiness Test

A ten minute check before an incident exposes the gaps

No	Test	Pass condition
1	Select a known event	Choose a person or vehicle movement from the previous day.
2	Find it	Retrieve the event by date, time and camera without installer help.
3	Check the image	Confirm the event question can be answered by day and, where relevant, at night.
4	Check time	Compare the displayed timestamp with a reliable reference and note any variance.
5	Check retention	Open the oldest available recording and record the actual date and time.
6	Export it	Create the system's native export and a viewing copy if the system supports one.
7	Play it elsewhere	Open the file on a separate authorised computer using supplied instructions.
8	Check context	Confirm camera name, site, date, time range and sequence are understandable.
9	Check access	Review named users, shared credentials and remote-app access.
10	Record the result	Assign every failure, owner and due date; repeat the failed test after correction.

Acceptance rule: the test passes only when an authorised staff member can retrieve, export and replay the correct event; the timestamp variance is understood; actual retention meets the approved requirement; and access or handling exceptions have named corrective actions.

PRACTICAL TOOL

Incident Export Record

Complete one record for each incident export. Keep it with the preserved export and do not overwrite the first exported files.

Record field	Response
Incident reference	
Date and time discovered	
Site and recorder	
Camera names or identifiers	
Requested incident period	
Actual exported period	
Exporter name and role	
Export date and time	
Native file names and format	
Viewing copy or player supplied	
Destination drive or secure location	
People receiving access or copies	
Reason for disclosure	
Known clock difference or system issue	
Later copies or transformations	
Approver and date	

CLOSING PERSPECTIVE

Test the Evidence Path Not Only the Camera

A CCTV system should be tested as a complete evidence path: scene, camera, network, recorder, storage, user access, export, playback and handover. A fault or weak control at any point can reduce the value of an otherwise good recording.

The monthly test is deliberately simple. It gives management evidence of what the system can do today, identifies dependence on one installer or employee and turns vague confidence into observable results. When the test fails, the corrective action may be a camera adjustment, better lighting, time synchronisation, more storage, user training, an export procedure or tighter access control.

The most useful question is not “Are the cameras working?” It is “Can an authorised person retrieve and explain a usable recording when the business needs it?”

This report is educational business-technology guidance. It is not legal advice and does not determine whether particular footage will be admissible or persuasive in any investigation, disciplinary process, insurance claim or court proceeding. Obtain appropriate legal and forensic advice for material or disputed incidents.