Data Retention & Deletion Policy

How long monitoring data is kept, how deletion is executed and evidenced, and what happens to your data when the engagement ends.

Status of this document. This is a vendor policy template issued for evaluation. It is not legal advice. If you intend to adopt it as your own organisation’s retention policy, have it reviewed and adapted by a qualified Nigerian legal practitioner against your actual processing, your sector obligations and any regulator undertakings you are already under. Where this document and your signed service agreement differ, the service agreement prevails. Wise Hustlers Technologies accepts no liability for reliance on this template as published.

Who this policy binds. In a typical deployment the client organisation is the **data controller** — it decides why the cameras exist and what happens to the data — and Wise Hustlers Technologies acts as **data processor**, operating the system on the controller's documented instructions. That means the retention periods below are *defaults and ceilings we recommend and enforce technically*; the controller sets the final schedule for its own site, and that schedule is recorded in the service agreement.

The split matters for breach handling too. Under NDPA s.40(1) a processor’s duty is to notify the controller on becoming aware; the **72-hour** clock in s.40(2) runs on the *controller’s* notification to the Commission, and s.40(3) requires immediate communication to affected individuals where the risk is high. Both parties must keep a record of every breach and its remedial action (s.40(8)).

1. The principle we apply

Monitoring data is kept for the shortest period that still serves the purpose it was collected for, and no longer. Where a client asks for a longer period, we ask what specific purpose requires it and record the answer, because “in case we need it” is not a retention justification that survives scrutiny.

Retention is enforced by a scheduled deletion job, not by an operator remembering to clear storage. There is no state in which a record silently outlives its schedule.

> **The regulatory ceiling.** Article 49(3) of the NDPC's GAID 2025 provides that where no timebound obligation applies, storage lapses **not later than six calendar months** after the original purpose has been accomplished — subject to retention genuinely needed for legal claims or due diligence. Every default in the table below sits well inside that. We state the ceiling because it is what a regulator will measure an extended retention period against, and because *"we keep it indefinitely in case we need it"* is not a position that survives contact with it.

---

2. Default retention schedule

These are the defaults applied unless the controller sets a different period in writing.

Data category	Default retention	Rationale
Event records Camera ID, timestamp, event type	30 days	Long enough for an incident to be noticed and investigated; short enough that a stale record is not sitting there indefinitely.
Recorded video Only where a controller enables recording	30 days	Aligns with the common insurance and internal-investigation window. Extended only against a stated purpose.
Biometric templates Only where matching is enabled	For as long as the individual remains on the controller's list, and deleted on removal	A template exists to serve a specific matching purpose. When the person leaves the list, the purpose ends.
Records subject to a legal hold	Until the hold is lifted	An identified incident under investigation. Placing and lifting a hold are both audit-logged and both require a named user.
Audit log entries	12 months minimum	The audit log must outlive the data it describes, or it cannot evidence who accessed something before it was deleted.
Administrator account records	Duration of the engagement, plus the agreed post-termination period	Needed to attribute historical access to a real person after they have left the role.

---

3. How retention is configured

- Retention is set **per camera**, not as a single system-wide value. A car park and a cash office have different risk profiles and should not be forced onto the same schedule.

- A change to a retention period is an administrative action performed by a named user and written to the audit log. Retention cannot be changed anonymously.
- Shortening a period takes effect on the next scheduled deletion run, which will then remove anything already beyond the new limit.
- Lengthening a period does not resurrect anything already deleted. Deletion is not reversible, by design.

---

4. How deletion is executed

1. A scheduled job runs at a defined interval and identifies every record past its retention period.
2. Records are deleted from primary storage.
3. Backup copies age out on their own defined cycle; the backup retention period is set so that a deleted record does not persist indefinitely in backup. Backup cycle length for your deployment is agreed at scoping and stated in the service agreement.
4. A deletion entry is written to the audit log recording what category was deleted and when. The entry does not reproduce the deleted content.

> **Deletion is a system behaviour, not a service request.** Routine expiry deletion does not require anyone at the client or at Wise Hustlers to raise a ticket, approve anything, or remember. That is the point: a retention policy that depends on human diligence is a retention policy that fails on a busy week.

---

5. Deletion on request

A data subject may ask the controller to erase data relating to them. Because the controller — not Wise Hustlers — owns that decision, the process is:

1. The request goes to the controller (the church, school, hotel, hospital or facility operator).
2. The controller decides whether the request is one it must honour, and instructs us.
3. We execute the deletion, and issue the controller written confirmation of what was deleted and when.

4. Both the instruction and the execution are audit-logged.

We do not act on an erasure request received directly from a third party without the controller's instruction, because doing so would mean destroying a controller's records on the say-so of someone whose identity and entitlement we are not positioned to verify.

---

6. What happens at the end of the engagement

Stage	Action
Notice period	The controller confirms which data it wants exported and in what format.
Export	Data is exported in the agreed format and transferred to the controller securely.
Verification	The controller confirms the export is complete and readable before anything is destroyed.
Deletion	All client data is deleted from primary storage; backups age out on the agreed cycle.
Certificate	A written deletion confirmation is issued to the controller, stating what was deleted and on what date.

> **Leaving is a documented process, not a commercial lever.** The export formats and the deletion procedure are agreed at the start of the engagement, in the contract, rather than negotiated at the point you want to leave.

---

7. Pilot deployments

A proof-of-concept pilot is time-boxed with a defined end date. At the close of the pilot, **all** data collected during it is deleted and a written deletion certificate is issued — whether or not the pilot converts into a permanent deployment. Pilot data is not retained as a head start on a future contract.

8. Review

This policy is reviewed when the deployment scope changes, when the controller changes its retention schedule, and otherwise annually. The version applying to your deployment is the one appended to your service agreement, which is the contractually operative document.