HARRISON COUNTY, INDIANA
ORDINANCE NO. 2026-____

AN ORDINANCE ESTABLISHING FISCAL ACCOUNTABILITY, CIVILIAN OVERSIGHT, DATA PROTECTION, AND CONSTITUTIONAL SAFEGUARDS FOR AUTOMATED VEHICLE SURVEILLANCE SYSTEMS (INCLUDING LICENSE PLATE READERS) USED BY HARRISON COUNTY GOVERNMENT

WHEREAS, the Fourth Amendment to the United States Constitution and Article 1, Section 11 of the Indiana Constitution guarantee the right of the people to be secure against unreasonable searches and seizures; and

WHEREAS, automated vehicle surveillance systems can record and aggregate the movements of every resident who drives in the County, and the long-term collection and retention of that location data raises serious constitutional and privacy concerns; and

WHEREAS, such systems also have legitimate value in recovering stolen vehicles, locating missing and endangered persons, and solving serious crimes, and it is the intent of this Ordinance to preserve those uses while preventing abuse; and

WHEREAS, misuse of these systems has been documented in other jurisdictions, including personal tracking, shared login credentials, and use beyond authorized purposes, and clear rules should be adopted before problems arise rather than after; and

WHEREAS, public spending on surveillance infrastructure should be openly debated and approved through the County Council's appropriation process;

NOW, THEREFORE, BE IT ORDAINED BY THE COUNTY COUNCIL AND BOARD OF COMMISSIONERS OF HARRISON COUNTY, INDIANA, AS FOLLOWS:

SECTION 1: DEFINITIONS

1. **"Automated Vehicle Surveillance System"** ("AVSS" or "System") means any camera, sensor, or device (fixed, mobile, portable, or drone-mounted), combined with software, that automatically captures, stores, indexes, or analyzes images or data of vehicles, license plates, vehicle descriptors, or vehicle movements. It includes automated license plate reader (ALPR) systems and any similar or successor technology, whether purchased, leased, operated, or accessed directly or indirectly by a County Entity.
2. **"County Entity"** means any County department, agency, office, or elected official (including the Sheriff's Office), and any employee, contractor, or task force participant acting for the County.
3. **"Access"** means any retrieval, search, viewing, or download of AVSS data, whether real-time or historical, and whether through a County interface, a vendor platform, a mutual aid agreement, a task force, or any other means.
4. **"Audit Log"** means a tamper-evident record of every Access that includes: the name and badge or ID number of the person accessing; the date, time, and duration; the search terms used (plate, vehicle description, location, and time range); the stated purpose; the associated case or incident number or the exigent justification; and any required supervisor approval.
5. **"Hot List"** means only official entries in government-maintained databases such as NCIC, IDACS, state stolen vehicle and warrant files, and Amber, Silver, or Missing Endangered Person

alerts.

6. **"Tracking"** means any Access that reconstructs or follows a vehicle's movements across more than one camera location or over a period longer than twenty-four (24) hours.

7. **"Preserved Data"** means AVSS data kept longer than the default retention period solely because of a documented trigger under Section 4. All other AVSS data is "Non-Preserved Data."

8. **"Exigent Circumstance"** means specific, articulable facts known to the officer at the time of Access showing an imminent threat of death or serious bodily injury to an identified person, where obtaining a warrant first is not reasonably practicable and the Access is limited to specific plates or descriptors. General claims such as "ongoing investigation" or "officer safety" do not qualify.

9. **"Vendor"** means any non-government entity, including any subcontractor, cloud host, or data processor, that stores, hosts, processes, or has access to AVSS data on the County's behalf (including Flock Safety or any similar platform).

10. **"Certified Equivalent Network"** means an outside AVSS network, agency, or jurisdiction that the Civilian Oversight Committee has certified under Section 6(e) as having privacy, retention, access, and audit standards at least equal to this Ordinance.

SECTION 2: FUNDING AND PUBLIC APPROVAL

(a) **Council Appropriation Required.** No County Entity shall purchase, lease, install, renew, or operate any AVSS using County funds unless the County Council has specifically appropriated funds for that purpose following a noticed public hearing. This Section is a condition on the use of County-appropriated funds and shall be applied to the fullest extent consistent with any independent statutory authority held by an elected official.

(b) **Outside Funding Treated the Same.** The following shall not be accepted or used for any AVSS purpose without specific Council approval at a public hearing: jail commissary funds, asset forfeiture proceeds, federal, state, or private grants, and donated or "gifted" equipment or services from individuals, businesses, homeowners associations, or other governments. Acceptance or use without prior approval is a violation of this Ordinance.

(c) **Impact Statement.** Before any hearing under this Section, the requesting County Entity shall file a written statement describing: total cost over five years; what data will be collected and who can access it; retention and sharing terms; vendor contract terms; and alternatives considered.

(d) **Existing Systems.** Within sixty (60) days after the effective date, each County Entity operating an AVSS shall report its cameras, vendor contracts, funding sources, and sharing arrangements to the Council and Committee. The Council shall hold a public hearing on each existing System within one hundred eighty (180) days after the effective date.

SECTION 3: CIVILIAN OVERSIGHT AND TRANSPARENCY

(a) **Civilian Oversight Committee.** A Civilian Oversight Committee ("Committee") is created, consisting of five (5) Harrison County residents appointed by the County Council to staggered three-year terms. No more than two members may have been employed in law enforcement within the past five years. Members serve without compensation. The Committee meets monthly during its first year and at least quarterly after that. Meetings are public, except for narrow closed sessions needed to protect an active investigation.

(b) **Powers.** The Committee, working with the County Auditor, has read-only access to all Audit Logs, System settings, retention settings, and deletion records, including Vendor-hosted records. The Committee may: request independent technical audits if funded by the Council; request

internal investigations; receive and decide complaints under Section 8; certify or decertify outside networks under Section 6(e); issue public reports and recommendations; and refer suspected violations to the Prosecuting Attorney.

(c) **Regular Log Review.** Each month the Committee shall review a random sample of Audit Log entries (at least five percent of Accesses, but not fewer than fifty or all entries if fewer) and shall also review every exigent-circumstance claim, every Tracking query, and every complaint or anomaly.

(d) **Staff Support.** The County Auditor shall provide clerical support to the Committee. This Ordinance does not require creating any new County position.

(e) **Public Dashboard.** The County shall maintain a public website updated at least quarterly showing: the number and general locations (by township or road segment) of AVSS units funded or accessed by the County; total Accesses; number of exigent uses and warrant-based Tracking queries; data-sharing requests granted and denied; violations found; deletion compliance; and the current list of Certified Equivalent Networks. No personal information or tactical details shall be published.

(f) **Annual Report.** The Committee and Auditor shall present a joint annual report to the Council in open session, published online at least ten (10) days beforehand, covering usage, audit findings, violations, discipline, Vendor compliance, and recommendations.

SECTION 4: DATA RETENTION AND DELETION

(a) **Thirty-Day Deletion.** All Non-Preserved Data shall be permanently deleted from all County and Vendor systems, including backups, no later than thirty (30) days after capture. Deletion shall be automatic through technical controls wherever possible.

(b) **Preservation Triggers.** Data may be kept beyond thirty days only for one of the following reasons, and only as long as the trigger lasts:

- an active criminal investigation or prosecution with a specific case number;
- a judicial warrant, subpoena, or court order; or
- a verified written preservation request from the person whose vehicle is involved, or that person's attorney.

Preserved Data shall be kept separate from other data, logged, and subject to the same access rules. It shall be permanently deleted within thirty (30) days after the trigger ends, unless a court orders otherwise.

(c) **No Workarounds.** Bulk export or download of System data is prohibited except in a documented active investigation with an Audit Log entry and supervisor approval. Any local copy is subject to the same deletion schedule.

(d) **Vendor Verification.** Vendors shall give the County a monthly written certification of deletion compliance, provide a means for independent verification, and purge data immediately on County demand.

SECTION 5: PERMITTED USES AND ACCESS STANDARDS

(a) **Permitted Purposes.** Access is allowed only for a legitimate law enforcement purpose tied to a Hot List alert, a stolen vehicle report, an active criminal investigation with a case number, a missing or endangered person, or an Exigent Circumstance.

(b) **Prohibited Uses.** Any Access for personal reasons, harassment, stalking, discrimination, monitoring of lawful First Amendment activity, predictive policing without individualized

suspicion, or any purpose not listed in subsection (a) is prohibited.

(c) **Hot Lists and Real-Time Alerts.** Real-time alerts are permitted for Hot Lists only. Officers must visually confirm a match before taking enforcement action based on an alert. Custom or agency-created watchlists are prohibited unless supported by individualized probable cause and, for ongoing tracking, judicial authorization.

(d) **Three Tiers of Access.**

- Real-time Hot List alerts: permitted, and logged.
- Case-linked search: a search for a specific plate or vehicle description at a specific place and time window tied to a particular reported offense is permitted with a case number and supervisor approval, and logged.
- Tracking: requires either (1) a signed judicial warrant based on probable cause, or (2) a documented Exigent Circumstance.

(e) **Exigent Documentation.** For any exigent Access, the officer shall document the specific facts in writing within twenty-four (24) hours and submit them to the Committee within seventy-two (72) hours. Failure to do so creates a presumption that the Access violated this Ordinance. The presumption may be overcome only by showing to the Committee that a true Exigent Circumstance existed and that the delay was beyond the officer's control. An unrebutted presumption is treated as a finding of violation under Section 8.

(f) **Everything Logged.** Every Access, including administrative and training queries, requires a complete Audit Log entry.

(g) **Emergencies Preserved.** Nothing in this Ordinance delays a response to an Amber, Silver, or Missing Endangered Person alert or an Exigent Circumstance.

SECTION 6: DATA SHARING AND JOINT PROGRAMS

(a) **Outside Networks.** County personnel shall not Access or obtain data from any outside AVSS network (another county, a state or federal agency, a task force, or a Vendor network) unless it is a Certified Equivalent Network, and each such Access must still meet every requirement of this Ordinance.

(b) **No Automatic Sharing.** The County shall not enable "national lookup," regional networks, or automatic data-sharing features in any Vendor platform unless the recipient is a Certified Equivalent Network and the Council approves the arrangement after a public hearing.

(c) **Outside Access to County Data.** Other agencies may access County AVSS data only under a Council-approved written agreement that requires equivalent standards and gives the Committee copies of their access logs. Blanket or ongoing access without such an agreement is prohibited.

(d) **Private and HOA Systems.** County Entities shall not integrate with or routinely access privately operated AVSS (such as HOA cameras) unless the operator agrees in writing to equivalent retention, logging, and access standards and the Council approves. This does not prevent an officer from requesting specific footage from a private party for a specific investigation, as with any witness video.

(e) **Certification.** The Committee may certify an outside network only by majority vote at a public meeting, after reviewing its written policies, retention practices, and audit capabilities, and only upon published written findings that its standards are equal to or stronger than this Ordinance. Lack of known violations is not a basis for certification. Certifications shall be reviewed annually and may be revoked at any time on evidence of non-compliance. County personnel must confirm a network's current certified status before each Access; a good-faith mistake is not a defense.

(f) **Task Forces and Federal Partnerships.** Joining a task force, joint operation, or federal

partnership does not exempt County data, personnel, or resources from this Ordinance, regardless of the program's own rules. Any such participation involving AVSS data must be disclosed to the Committee in advance, with the program's data-sharing rules and participating agencies, and approved by the Council after a public hearing.

SECTION 7: VENDOR CONTRACT REQUIREMENTS

Every AVSS Vendor contract shall, as a condition of validity, include at least the following:

- automatic hard deletion under Section 4, with no ability for the County or Vendor to extend retention except through the audited preservation process;
- independently verifiable read-only access for the County Auditor and Committee to logs, settings, and deletion records;
- a ban on the Vendor keeping, copying, selling, or sharing County data, or using it for AI or machine-learning training or commercial profiling, beyond what is needed to serve the County (except sharing allowed under Section 6);
- County ownership and control of all data, with the Vendor acting only as custodian;
- County rights to terminate and require immediate purge on material breach or violation of this Ordinance, with Vendor responsible for transition and verification costs;
- storage and processing within the United States;
- an annual independent security and compliance audit, or the County's right to commission one at Vendor expense; and
- flow-down of every requirement in this Section to all subcontractors and downstream processors, with the primary Vendor liable for their compliance and required to disclose them on request.

Existing contracts shall be amended to comply within ninety (90) days after the effective date, or the County shall exercise its rights of termination or non-renewal at the earliest time the contract allows.

SECTION 8: ENFORCEMENT AND REMEDIES

(a) **Individual Sanctions.** Any County employee, official, or contractor who knowingly or intentionally Accesses, uses, shares, or permits use of an AVSS in violation of this Ordinance shall be subject to immediate loss of System access; discipline up to and including termination; and referral to the Prosecuting Attorney for review under IC 35-44.1-1-1 (Official Misconduct) and any other applicable law. To the fullest extent the law permits, the County shall not defend or indemnify a person for a knowing or intentional violation.

(b) **Agency Consequences.** After notice and an opportunity to be heard, the Council may suspend or end funding for the AVSS program of any County Entity that shows a pattern of violations or systemic non-compliance.

(c) **Data Obtained in Violation.** The County shall not use data obtained in material violation of this Ordinance in any County administrative or disciplinary proceeding. The Committee shall notify the Prosecuting Attorney of any such violation so that disclosure can be made as required by law.

(d) **Training.** Every person with System access must complete annual training on this Ordinance, constitutional limits, and proper justification before access is granted or renewed. Training records are public.

(e) **Complaints.** Any Harrison County resident who believes their vehicle data was accessed in violation of this Ordinance may file a written complaint with the Committee. The Committee shall investigate, may hold a hearing, and may order corrective action, including confirmation that data has been deleted, referral for discipline or prosecution, and public disclosure of findings

(without personal information). The Committee shall issue a written decision within sixty (60) days after a complete complaint is filed.

(f) **Civil Remedies Preserved.** This Ordinance does not remove any right to seek relief in court for a knowing violation, including declaratory or injunctive relief and actual damages. Any such action remains subject to the Indiana Tort Claims Act (IC 34-13-3) and other applicable law. This subsection does not create new governmental liability beyond what state law already allows.

(g) **No Retaliation.** No County Entity shall retaliate against an employee who reports a suspected violation of this Ordinance in good faith.

SECTION 9: GENERAL PROVISIONS

(a) **Construction.** This Ordinance shall be interpreted to protect individual privacy and constitutional rights. Any ambiguity shall be resolved in favor of greater privacy.

(b) **Severability.** If any provision is held invalid or unenforceable, including because it conflicts with an official's independent statutory authority or with the Indiana Tort Claims Act, that provision shall be reformed to the minimum extent needed to comply with law and the rest of this Ordinance shall remain in effect.

(c) **Effective Date and Compliance.** This Ordinance takes effect sixty (60) days after passage. Existing Systems and contracts shall be brought into full compliance, including deletion of data held past the limits in Section 4, within ninety (90) days after the effective date, or be discontinued.

(d) **Review.** The Council shall review this Ordinance, with the Committee's recommendations, no later than two years after the effective date.

(e) **Conflicting Provisions.** Any prior ordinance, resolution, or policy of a County Entity that conflicts with this Ordinance is superseded to the extent of the conflict.

PASSED AND ADOPTED by the County Council of Harrison County, Indiana, this _____ day of _____, 2026.

_____ _____

Council President Council Member

PASSED AND ADOPTED by the Board of Commissioners of Harrison County, Indiana, this _____ day of _____, 2026.

_____ _____

Commissioner Commissioner

_____

Attest: County Auditor