

MEMORANDUM

To: Sponsors of the proposed ATESD Ordinance Drafting Committee (RTM Agenda Item 6, Aug. 24, 2026)

From: Emily Hau, Fairfield resident

Date: August 19, 2026

Re: Baseline vendor governance requirements for the speed-camera program

Why this memo. The camera vendor holds a year of residents' license-plate data, and every ticket payment passes through a bank account the vendor controls before the town is paid. On August 17 the town could not say where resident data is stored; deletion was "that's what I'm told." Each item below is standard commercial vendor-management practice, adoptable by ordinance for this and any future data-handling vendor. A SOC 2 Type II should remain the baseline; these supplement it:

1. **Vendor security questionnaire (SIG Core or equivalent).** Before renewal and annually after, the vendor completes a standardized assessment answering the town's questions about its security, not just the ones its own auditor chose.
2. **Business continuity and disaster recovery plan.** The vendor's BCP/DR plan with numeric, town-approved recovery objectives (RTO/RPO) carrying remedies if missed, evidence it has been tested, immutable backups in a geographically separate region, and the town's data retrievable by the town at all times (escrow or scheduled export). Citation and appeal deadlines are tolled during any outage, and no resident loses appeal rights or incurs a late fee because of a system or vendor failure.
3. **Service-level agreements.** Contractual SLAs for system uptime, citation processing time, payment posting, and support response, with remedies when missed. Today the contract obligates residents' deadlines but almost none of the vendor's.
4. **Support policy, hours, and escalation.** Written support hours, response times, and a named escalation path where Fairfield police and parking staff reach a human, not a portal. On August 17, questions were repeatedly answered with "it's for the company to answer." Someone there should.
5. **Change and release management.** How releases are tested, approved, and communicated to the town before going live, and how errors are reported. Citations went out with wrong fine amounts during rollout, an error the town's CFO valued at roughly \$104,200. The process that allowed it has never been documented.
6. **Incident response and breach notification.** A written incident-response plan; preliminary notice to the town within 24 hours of discovery or reasonable suspicion, with daily updates; and notice to affected residents. Liquidated damages per exposed record and per day of late notice; the vendor bears all forensic, notification, and credit-monitoring costs; and exposed residents are refunded all fines and fees paid.
7. **Data residency and subprocessors.** Where resident data is physically stored (state and country), every subprocessor that touches it, including payment and lockbox providers, and town approval before either changes.
8. **Deletion certification.** Automated purge built into the software plus written quarterly certification that it ran, covering every copy: production, replicas, backups, archives, logs, and subprocessors, with a narrow, documented legal-hold exception that expires. The ordinance's 30-day rule, the contract's 90-day clause, and the one-year retention described on August 17 must be reconciled into one rule residents can read. State law (C.G.S. § 14-307d) requires the state's model privacy policy to establish internal audit requirements; has that audit ever been performed?
9. **Rights printed on the citation.** Every material right appears on the citation itself, in plain language: the appeal window, any extensions (e.g., leased vehicles), and how to contest. Residents should not discover their rights on a website or a vendor phone line.
10. **Independent assessment and right to audit.** An end-to-end assessment of the whole program, commissioned and paid for by the town, covering controls, payment and citation workflows, retention, backups, and incident response. An audit the vendor pays for is the vendor's audit.
11. **Access controls and an access log.** Who (by role) can access resident data; MFA and encryption in transit and at rest; least privilege, separate admin accounts, prompt revocation on termination; tamper-evident logs of every access and every change to a citation, fine, or appeal status, including the prior value; chain-of-custody verification so the evidentiary image shown at a hearing is provably the one captured; background checks and training for staff handling DMV records; and public disclosure of who can access the data and a summary log of who has.
12. **Financial viability.** Annual financial statements or an equivalent assurance of solvency; if the vendor fails, the town's money is in an account the vendor established and controls.
13. **Corporate governance and key personnel.** The vendor's own code of ethics and code of conduct on file with the town, plus notice of executive-team changes, a risk signal the town should see, not discover.
14. **Cyber insurance.** Cyber liability coverage at stated minimums with the Town of Fairfield named, so a breach does not become a taxpayer expense.
15. **Annual public transparency report.** Once a year, in plain language: data collected, retention as practiced, deletion certifications, audits, SLA performance, incidents, and any outside-agency access.

APPENDIX — Contract-grade specifics for the Town Attorney

Page 1 sets the policy; these six provisions make it enforceable, adaptable into the vendor agreement at renewal or sooner by amendment. The contract should also require annual delivery of the vendor's current SOC 2 Type II report itself, with scope, exceptions, and complementary user-entity controls. Posture note for counsel: these are opening positions, stated at full strength on purpose; some, like the full-refund breach remedy, may land as a remedy schedule set by ordinance. Negotiate down from the residents' position, not up from the vendor's.

A. Data ownership, purpose limitation, and prohibited uses. All images, video, metadata, and citation records are the sole and exclusive property of the Town; the vendor acts only as a service provider processing data on the Town's behalf. The vendor may use Town data solely to perform this contract, and may not sell, license, disclose, monetize, aggregate, analyze for unrelated purposes, use to train AI or machine-learning models, or combine with other datasets, nor permit any third party to do so. The vendor shall notify the Town before responding to any subpoena, warrant, or other government demand for Town data unless legally prohibited, and may not voluntarily disclose Town data to civil litigants, private parties, or out-of-state agencies without a court order. Audit logs, configuration history, incident records, and program documentation are Town records too: Town-owned, retained per the Town's records-retention schedule and applicable law, and delivered at termination. This mirrors the ordinance's own § 102-15 disclosure limits and makes them contractual.

B. Vulnerability management and penetration testing. Continuous vulnerability management with defined remediation deadlines for critical and high-severity findings; annual independent penetration testing with results summarized to the Town; notice of any vulnerability materially affecting Fairfield's data or citations; and remediation verification. Field hardware counts too: encrypted storage on the camera units, notice within 12 hours of theft or tampering, and calibration and maintenance records linked to citations, since the ordinance (§ 102-10) requires every citation to state the date of the device's most recent calibration check. If system integrity cannot be verified after an incident, citation issuance stops until integrity is restored and verified.

C. Subprocessor flow-down liability. Every subprocessor, including cloud, payment, and lockbox providers, must be contractually bound to protections at least as stringent as the vendor's own, and the vendor remains fully liable for its subprocessors' acts and omissions. Subprocessor changes require the Town's prior written approval, which may be withheld for security, privacy, financial, or legal-compliance reasons. "The breach happened at our subcontractor" is not a defense the Town should ever hear.

D. Custody of public funds. Resident payments are held in a dedicated, segregated account for the benefit of the Town, are not vendor assets, and are not subject to vendor creditors. No commingling; daily reconciliation visible to the Town; a defined remittance schedule; dual controls on withdrawals; and audit rights over the account. Standard cybersecurity audits do not examine banking arrangements or the custody of public funds.

E. Termination, portability, and transition. On termination for any reason: a complete export of Town data in open, non-proprietary formats (CSV or JSON for records, standard image and video formats for evidence) with schema and documentation sufficient for a successor vendor to use it, at no extraction, licensing, or conversion fee; continued system access through a defined transition period; migration assistance; turnover of Town-owned configuration; and certified deletion within 30 days after successful transition, absent a documented legal hold. The Town should be able to hand its data to Vendor B on Monday after leaving Vendor A on Friday. And Town access to Town data may never be suspended over a payment or contractual dispute.

F. Indemnification, insurance specifics, and liability-cap carveouts. Here the current agreement itself is the exhibit. Its indemnification (§ 12) is broad but runs to Altumint's own officers, agents, and employees; it should extend expressly to subprocessors' acts and regulatory costs. Its insurance section (§ 11) requires general liability, property, auto, and workers' compensation, but no cyber or privacy-breach coverage at all, for a vendor whose entire product is data; counsel should require cyber coverage with stated minimums covering breach response, ransomware, regulatory and forensic costs, and business interruption, with annual proof and notice of cancellation or material reduction. And § 11 caps Altumint's cumulative liability at \$5,000,000 while excluding all punitive, incidental, indirect, or consequential damages, the categories vendors typically argue breach costs fall into. The security, privacy, funds, and liquidated-damages obligations in this memo must be expressly carved out of that cap and exclusion, or existing boilerplate defeats every remedy above the moment there is a dispute.

Sources: C.G.S. §§ 14-307b–14-307e; Fairfield Town Code ch. 102, art. II (incl. §§ 102-7, 102-15); executed Town–Altumint Photo Enforcement Services Agreement (RFP #0225-60R), incl. §§ 8, 11, 12, 19 and Schedule A; Aug. 2026 RTM backup packet (CFO memo); Aug. 17, 2026 RTM informational meeting.

One sentence for the committee's use: a SOC 2 is an independent auditor testing a scope selected with the vendor; the SIG is the town asking the questions the town needs answered. — Emily Hau · mrsemilyhau@gmail.com · fairfieldspeedcams.netlify.app