Initiative 2025-2026 #272
Creation of Automation Mitigation Enterprise

Received by Legislative Council Staff
3/6/26 at 5:21 AM

STATE OF COLORADO

BILL 2

SECURE DIGITAL INFRASTRUCTURE AND ENFORCEMENT ACT

A Bill for an Act Concerning Secure Enforcement Infrastructure, the Colorado Trust of Unique and Identifying Information, Facility Chain-of-Command Incident Reporting Protocols, and Secure Inmate Grievance and Incident Submission Systems

AMPLIFY Act — Bill 2 of 3 | Title 10, Article 10 | AMPLIFY Act

ENACTING CLAUSE & SINGLE SUBJECT

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns the establishment of statewide secure verification, accountability, and safety infrastructure for systems that process or control protected Digital Soul interests or administer public functions using Emergent Automation, including air-gapped custodial trust operations, incident-detection and monitoring standards, and integrity protections for public-service eligibility and detention life-safety reporting.

Construction; no enterprise finance in this act. References in this act to the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) or to Enterprise Mitigation revenues are for coordination and cross-reference only. This act does not levy, authorize, or administer enterprise assessments or charges. This act is intended to be operable independently.

SECTION 1. LEGISLATIVE DECLARATION

(1.5) The general assembly further finds and declares that secure administration of resident Digital Soul protections and public services requires a unified infrastructure of: (a) cryptographic verification and custodial containment for protected hashes and audit artifacts; (b) outcome-based safety monitoring and incident reporting for Emergent Automation systems interfacing with public functions; and (c) integrity safeguards preventing item-level identifiers and transactional telemetry from being repurposed for prohibited

profiling. All provisions of this act are necessarily and properly connected to that unified purpose.

(1) The general assembly finds and declares that: (a) Colorado residents possess enforceable digital property and sovereignty rights that require secure, neutral, and constitutionally compliant enforcement infrastructure; (b) Automated systems can generate false positives, discriminatory outcomes, and irreversible harms unless enforcement is constrained by due process, human verification, and auditable cryptographic controls; (c) State-held fiduciary cryptographic custody and air-gapped storage systems strengthen Fourth Amendment protections by reducing third-party seizure risk; (d) Physical disconnection mechanisms are necessary in designated sanctuary and pre-digital mechanical assets to preserve analog access; and (e) Detention facilities require non-circumventable chain-of-command reporting infrastructure to protect residents, staff, and the public interest.

(2) It is the intent of the general assembly that this Act: (a) Establishes the Division (ODO) to oversee ethics, investigations, and resident protection; (b) Creates the Colorado Trust of Unique and Identifying Information as the air-gapped state verification and audit infrastructure and Colorado Automation Mitigation Custodial Architecture; (c) Implements a Triad Review Panel and Judicial Cryptographic Token system to ensure due process; (d) Establishes the Panel and two-step verification protocol for algorithmic flags; (e) Mandates a statewide Non-Networked Isolation Protocol; and (f) Establishes the Facility Chain-of-Command Incident Reporting System and Secure Inmate Grievance and Incident Submission System for detention facilities.

SECTION 2. In Colorado Revised Statutes, add article 10 to title 10 as follows:

ARTICLE 10 — SECURE INFRASTRUCTURE AND JUSTICE

10-10-101. ***Definitions.***

As used in this article 10, unless the context otherwise requires:

(1) "Air-gapped" means physically isolated from the public internet and from any external network such that no data can be transmitted to or from the system except through controlled, logged, and authenticated transfer procedures.

(2) "Non-Networked Isolation Protocol" means a mandatory hardware-level circuit-break and physical disconnection capability for covered Emergent Automation systems, providing resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions, with enhanced requirements in designated sanctuary and pre-digital mechanical assets.

(3) "The Colorado Trust of Unique and Identifying Information" or "The Trust" means the proprietary, decentralized, and air-gapped state storage and audit environment

established under this article, operating as the state verification and audit infrastructure — the primary sovereign repository and funding trigger mechanism for the Enterprise Mitigation Revenue established under article 20 of title 24. The Trust is designed to support zero-knowledge audit proofs, contraband-data compliance verification, and secure Digital Soul mitigation custodial services. The Trust operates strictly as a blind fiduciary repository. It is structurally prohibited from continuous data ingestion and may only house cryptographic Resident Identity Verification Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

(4) "state verification and audit infrastructure" means the function of the Colorado Trust of Unique and Identifying Information as the primary cryptographic verification and triggering mechanism for Enterprise Mitigation revenue events, including the Data Tap routing that distinguishes Tier 1 (anonymous) data events from Tier 2 (identifying) data events for purposes of Base Dividend and Premium Royalty calculations under article 20 of title 24.

(5) "The Panel" means a paid, human-in-the-loop workforce of temporary civic workers tasked with verifying algorithmic flags and compliance events under the two-step verification process.

(6) "Contraband Data" means any data ingested, processed, stored, trained upon, or used without a valid, cryptographically verifiable Decentralized Identity Verification Protocol or in violation of an Intake Firewall.

(7) "Colorado Automation Mitigation Custodial Account" means state-held encrypted custody of Digital Soul or resident audit artifacts in a fiduciary capacity, utilizing cryptographic access controls and key management to prevent unauthorized access and to require judicially authorized procedures for unmasking.

(8) "Judicial Cryptographic Token" or "JCT" means a time-bound, rotating session token serving as the lock-and-key mechanism authorized by a Triad Review Panel for the limited purpose of unmasking or accessing protected audit data.

(9) "Shadow Person Output" means an anonymized tokenized audit artifact that omits facial and direct identifiers, used for initial verification by the Panel to preserve privacy.

(10) "Triad Review Panel" means a mandatory oversight body consisting of a prosecutor, a defense attorney, and a magistrate serving as the authorization authority for high-level data access, unmasking, and intensive audits.

(11) "Two-step verification" means the process by which two independent, randomized verifiers confirm an alleged contraband-data event or compliance violation before any adverse action may issue.

(12) "CSAM" means any visual depiction of sexually explicit conduct involving a minor, as defined by applicable state and federal law.

(13) "Synthetic CSAM" means any computer-generated or emergent automation-generated depiction that depicts a minor engaging in sexually explicit conduct, regardless of whether it is derived from an identifiable real minor.

(14) "Zero-Tolerance Compute Mandate" means the strict-liability operational requirement that prohibits any covered entity from using compute resources to generate, transform, distribute, store, train on, or otherwise process CSAM or Synthetic CSAM.

(15) "Covered entity" or "covered operator" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides a covered emergent

automation system in Colorado, or that commercially delivers such a system to or targets Colorado residents.

(16) "Facility Chain-of-Command Incident Reporting System" means the verifiable, non-circumventable chain-of-command incident reporting, verification, and escalation system for detention facilities established under section 10-10-150.

(17) "Civic Enforcement Access Terminal" or "Jail Kiosk" means the secure, tamper-evident inmate-facing terminal deployed under section 10-10-151 for resident reporting, grievance intake, legal access, and Non-Circumventable Incident Reporting incident submissions.

(18) "Master Log" means the immutable, tamper-evident, continuously maintained record of all Non-Circumventable Incident Reporting incident submissions, verification actions, escalation decisions, and warden determinations required under section 10-10-152.

(19) "Three-Strike Escalation" means the mandatory review and escalation protocol under section 10-10-153 by which an unresolved or disputed Non-Circumventable Incident Reporting report progresses through three independent review levels culminating in final warden determination.

(20) "Resident Identity Verification Hash" means a cryptographic one-way hash of a resident's Digital Soul identifiers stored within the Colorado Trust of Unique and Identifying Information, used for zero-knowledge verification without exposing underlying resident data.

(21) Delegated system; operator responsibility. Any model, automated system, tool, contractor, processor, or service operating under the authority, license, or delegation of a covered entity is deemed an extension of that covered entity for purposes of duties, enforcement, and liability under this article.

(22) "Verified Incident Record" or "VIR" means a verifiable, non-destructive incident record created only after two-step verification, consisting of the underlying source record references, the Shadow Person Output or other minimized artifact reviewed, the identities (or authenticated reviewer IDs) of both independent verifiers, timestamps, the verification outcome (sustained, not sustained, or inconclusive), and any escalation or unmasking authorization issued under this article.

(23) "Adverse action" means any action that materially affects a person's liberty, legal status, access to goods or services, employment, housing, credit, benefits, education, medical care, custody status, detention conditions, account access, or that initiates, escalates, or materially influences a referral to law enforcement, issuance of a citation, trespass order, detention, or similar enforcement consequence.

(24) "Authorized Successor Data Designation" means an encrypted, resident-governed, append-only record container within or interoperable with the Trust, designed to preserve a durable record for a household or family group, subject to multi-party authorization for critical actions, non-destructive corrections, and continuity/portability requirements under section 10-10-108.6.

THE COLORADO TRUST OF UNIQUE AND IDENTIFYING INFORMATION — state verification and audit infrastructure

10-10-103. The Colorado Trust of Unique and Identifying Information — Sovereign Air-Gapped Storage — state verification and audit infrastructure — Zero-Knowledge Audits.

(1) The state shall establish and maintain the Colorado Trust of Unique and Identifying Information as an air-gapped, decentralized storage and audit environment, operating as the state verification and audit infrastructure — the sovereign origin point and primary verification mechanism for all Enterprise Mitigation revenue events authorized under article 20 of title 24.

(2) The Trust shall: (a) support receipt and verification of zero-knowledge audit proofs for contraband-data compliance without requiring public disclosure of proprietary source code, model weights, or trade secrets; (b) maintain immutable audit logs for all access attempts and all JCT authorizations; (c) serve as the cryptographic trigger mechanism for Data Tap financial routing events, distinguishing Tier 1 anonymous data events from Tier 2 identifying data events for purposes of Base Dividend and Premium Royalty calculations; (d) provide resident-facing access through the myColorado platform for Resident Identity Verification Hash registration, certificates, notices, and audit attestations, as authorized by law.

(3) Data Tap Financial Routing — state verification and audit infrastructure trigger function. The Trust shall implement the Data Tap as follows: (a) Tier 1 Data Events. When the Trust verifies a covered data transaction involving anonymized or de-identified data as defined by rule, the Trust shall generate a Tier 1 Data Tap signal. The Tier 1 signal triggers a Base Dividend calculation into the Colorado Automation Mitigation Trust under article 20 of title 24. Tier 1 events carry the lower assessment rate established under section 24-20-116(2)(b). (b) Tier 2 Data Events. When the Trust verifies a covered data transaction involving personally identifying information, distinct persona links, or Digital Soul attributes that can identify or re-identify a resident, the Trust shall generate a Tier 2 Data Tap signal. The Tier 2 signal triggers a Premium Royalty calculation routed directly to the resident's Resident Automated Mitigation Account via the Trust. Tier 2 events carry the higher assessment rate established under section 24-20-116(2)(a).

(4) The ODO shall establish certification standards for entities that integrate with the Trust, including secure transfer procedures, logging, and key management.

(5) No continuous ingestion. The Trust is structurally prohibited from continuous data ingestion. It may only house Resident Identity Verification Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

10-10-104. Colorado Automation Mitigation Custodial Account — Fourth Amendment Protection Architecture.

(1) The state may hold encrypted Digital Soul and resident audit artifacts in Colorado Automation Mitigation Custodial Account.

(2) Mitigation custodial custody under this section: (a) does not transfer title or beneficial ownership of resident property to the state; (b) requires adherence to strict fiduciary duties, including confidentiality, minimization, and purpose limitation; (c) is designed to reduce third-party seizure risk and to require judicially supervised procedures for access.

(3) No state employee shall access protected data held in mitigation custodial accounts except pursuant to a valid Judicial Cryptographic Token issued under

section 10-10-105, and only to the minimum extent necessary for the authorized purpose.

TRIAD REVIEW PANEL AND JUDICIAL CRYPTOGRAPHIC TOKEN

10-10-105. ***Triad Review Panel — Judicial Cryptographic Token — Due Process.***

(1) The Triad Review Panel is hereby established. The chief judge of each judicial district shall designate magistrates to serve, and the ODO shall maintain rosters of qualified prosecutors and defense attorneys.

(2) A Judicial Cryptographic Token may issue only upon: (a) a sworn application stating the specific scope of data access sought, the factual basis for the request, and the minimization procedures to be employed; (b) a finding by the Triad Review Panel that the request is narrowly tailored and supported by probable cause or other applicable legal standard; (c) a determination that less intrusive means are unavailable or insufficient.

(3) Each JCT shall: (a) be time-limited and scope-limited; (b) permit only the minimum unmasking or access necessary for the authorized purpose; (c) generate immutable logs within the Trust.

(4) The ODO shall implement standardized notice procedures, including delayed notice where authorized by court order.

(5) Community Supervision — Court-Ordered Condition; Limited Whereabouts Access. Notwithstanding the JCT requirements of this section, limited, real-time access to a resident's whereabouts data by the Department of Corrections or the Judicial Department is authorized only when such access is an express condition of supervision imposed by a court, parole authority, or other lawful supervising authority. Tiered authorization: (I) Standard supervision requires concurrent digital authorization of both the assigned supervising officer and the officer's direct supervisor. (II) Intensive supervision requires the digital authorization of the assigned supervising officer. Access shall be limited to the minimum data necessary and shall not include bulk historical location history beyond a narrowly tailored time window. Any whereabouts data unmasked shall automatically generate an immutable audit log within the Trust.

(Y) Emergency guardian tether for minors — active missing-child alert. When a minor resident is the subject of an active, verified Colorado Bureau of Investigation AMBER Alert or Endangered Missing Alert, a custodial parent or lawful guardian may authorize an emergency decryption tether for the limited purpose of locating the minor. The tether shall automatically expire at the earliest of: (I) cancellation of the alert; (II) confirmation the minor has been recovered; or (III) twenty-four (24) hours after activation, unless renewed pursuant to an active alert. Any data unmasked shall generate an immutable audit log within the Trust.

(Z) Voluntary kinship tether for adults — life-safety activation; no state key custody. Two adult residents may, by mutual consent, establish a voluntary kinship tether through a peer-to-peer authorization method. The State and The Trust shall not hold persistent decryption keys for voluntary kinship tethers. A request to activate may be honored only during a verifiable life-safety emergency corroborated by independent objective signals.

Any activation request shall immediately trigger an unblockable, device-level notification to the targeted resident, who retains an always-on veto. Default disablement applies where there is an active civil protection order between the parties.

EYE IN THE SKY — CHAIN-OF-COMMAND REPORTING SYSTEM

10-10-150. Non-Circumventable Incident Reporting System — Purpose — Architecture — Non-Circumventability.

(1) Purpose. The general assembly finds that detention facilities present acute, demonstrable civil-liability and public-safety risks arising from unreported misconduct, retaliatory silencing of residents, and inadequate chain-of-command accountability. The Non-Circumventable Incident Reporting System is hereby established as a verifiable, non-circumventable digital chain-of-command for sensitive conduct reporting within detention facilities, ensuring that every incident report is verified, logged, escalated appropriately, and resolved with documented finality.

(2) Architecture. The Non-Circumventable Incident Reporting System shall: (a) receive incident reports submitted by residents through the Civic Enforcement Access Terminal under section 10-10-151 or by staff through authenticated duty-status terminals; (b) automatically verify submission integrity using cryptographic time-stamps, tamper-evident hashing, and kiosk session logs stored in the Colorado Trust of Unique and Identifying Information; (c) route verified reports to the appropriate level of the facility chain of command based on the category and subject of the report as established in subsection (3); (d) automatically escalate any report that implicates a supervisor, official, or staff member to that person's direct superior within the chain of command; and (e) log every action, routing decision, escalation event, acknowledgment, and resolution in the Master Log under section 10-10-152.

(3) Report routing — automatic escalation. (a) Reports implicating a staff member who is not in a supervisory role shall be routed to that staff member's direct supervisor for initial verification and determination. (b) Reports implicating a supervisor shall bypass that supervisor entirely and be routed automatically to the supervisor's direct superior. (c) Reports implicating a facility commander or warden-level official shall be routed automatically to the regional administrator or cognizant external oversight authority. (d) No implicated official, supervisor, or staff member may access, modify, suppress, delay, or resolve a report that names them as a subject.

(4) Non-circumventability mandate. The Non-Circumventable Incident Reporting System shall be designed and operated so that: (a) no individual within the chain of command may unilaterally close, delete, suppress, or reroute a verified incident report without a documented determination entered into the Master Log; (b) the system shall detect and flag any attempt to access or modify a report by a named subject; and (c) the ODO shall receive an automatic notification of any flagged circumvention attempt within one (1) hour.

(5) Integration with the Trust. All Non-Circumventable Incident Reporting incident data, routing logs, escalation records, and warden determinations shall be

encrypted and stored in the Colorado Trust of Unique and Identifying Information as Static Incident Artifacts pending resolution. Upon final resolution, artifacts shall be archived in the Master Log with access restricted to authorized reviewers pursuant to a JCT.

10-10-151. Civic Enforcement Access Terminal — Jail Kiosk Integration — Resident Reporting Rights.

(1) Establishment. Each detention facility that opts into the pilot under section 10-10-190 shall deploy at least one Civic Enforcement Access Terminal per housing unit, accessible to all residents without requiring staff escort or prior authorization.

(2) Resident reporting functions. The Civic Enforcement Access Terminal shall enable a resident to: (a) file an incident report against another resident for misconduct, safety, or welfare matters; (b) file an incident report against a staff member, supervisor, or official for misconduct, abuse, retaliation, civil rights violations, or other conduct of concern; (c) submit grievances and access legal resources; (d) access no-cost video and audio communications with approved family members, guardians, and legal counsel; and (e) access the Non-Circumventable Incident Reporting submission interface for anonymous or identified reporting.

(3) Anonymous reporting option. A resident may elect to submit a report anonymously through the Non-Circumventable Incident Reporting interface. The kiosk shall implement a one-way anonymization method that: (a) prevents the facility or staff from identifying the submitting resident; (b) preserves a sealed resident-identity record within the Trust accessible only pursuant to a JCT for purposes of verifying report authenticity and preventing abuse; and (c) notifies the resident that anonymous reports may receive different procedural treatment but shall not be suppressed solely on the basis of anonymity.

(4) Anti-retaliation architecture. (a) Any action taken against a resident within seventy-two (72) hours of the resident submitting an Non-Circumventable Incident Reporting or kiosk report shall automatically generate a retaliation-flag entry in the Master Log. (b) The retaliation-flag entry shall be routed to the ODO for review within twenty-four (24) hours. (c) No adverse action against a resident shall be processed through an automated system without human verification under section 10-10-108.5 where a pending retaliation flag exists.

(5) Accessibility and analog fallback. Every Civic Enforcement Access Terminal shall: (a) offer interface options in the primary languages spoken by the facility population; (b) provide accessibility accommodations including audio narration and large-print modes; and (c) maintain a paper-based grievance fallback intake process at parity of timeliness and quality with kiosk submission.

10-10-152. *Master Log — Immutable Record — Retention — Access.*

(1) Creation and maintenance. The facility shall maintain a Master Log of all Non-Circumventable Incident Reporting and Civic Enforcement Access Terminal activities, stored as immutable artifacts within the Colorado Trust of Unique and Identifying Information. The Master Log is a permanent, non-deletable record. No

entry in the Master Log may be altered, overwritten, or removed by any facility staff, administrator, or contractor.

(2) Required Master Log entries. For every incident report submitted through the Non-Circumventable Incident Reporting System or Civic Enforcement Access Terminal, the Master Log shall record: (a) the date, time, and kiosk terminal identifier of submission; (b) the category of the report and the identity of the subject of the report, where known; (c) each routing and escalation event, including timestamps and the identity of each reviewer; (d) each determination, acknowledgment, response, and resolution action taken, with the identity of the decision-maker and the stated basis; (e) any retaliation flag events as described in section 10-10-151(4); (f) any Three-Strike escalation events under section 10-10-153; and (g) final warden determination and disposition.

(3) Retention. Master Log records shall be retained for a minimum of ten (10) years and shall not be purged, destroyed, or redacted except pursuant to a court order or as required by applicable law, provided that purging shall be logged with the reason and authority. Records pertaining to unresolved matters shall be retained indefinitely until final resolution.

(4) Access. Access to Master Log records shall be governed by the JCT process under section 10-10-105, except that: (a) the submitting resident may access their own submission and the resolution record; (b) the ODO may access all records for oversight, audit, and enforcement purposes; and (c) records relevant to active litigation shall be made available pursuant to lawful process.

10-10-153. ***Three-Strike Escalation Protocol — Review Levels — Warden Final Determination.***

(1) Purpose. The Three-Strike Escalation Protocol ensures that every Non-Circumventable Incident Reporting incident report receives at minimum three independent levels of review before final determination, preventing single-point suppression of credible reports.

(2) Strike One — Initial supervisor review. Upon routing to the initial reviewer under section 10-10-150(3), the reviewer shall have five (5) business days to: (a) acknowledge receipt in the Master Log; (b) conduct an initial investigation consistent with facility policy and this article; and (c) enter a written determination — sustained, not sustained, or inconclusive — into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Two.

(3) Strike Two — Secondary supervisor escalation. Upon Strike Two, the report is automatically routed to the next level of the chain of command above the Strike One reviewer. The Strike Two reviewer shall have five (5) business days to: (a) independently review the report and the Strike One record; (b) conduct any additional investigation; and (c) enter an independent written determination into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Three.

(4) Strike Three — Warden final determination. Upon Strike Three, the report is automatically and irrevocably routed to the facility warden or, if the warden is implicated, to the regional administrator. The warden or regional administrator shall have ten (10) business days to: (a) independently review the full record; (b) enter a final written determination into the Master Log; (c) specify any corrective actions, disciplinary

proceedings, or referrals to external authorities; and (d) provide written notice to the submitting resident of the final determination, consistent with applicable privacy and safety considerations.

(5) ODO notification. The ODO shall receive automated notification upon: (a) any Strike Two or Strike Three trigger event; (b) any warden final determination; and (c) any retaliation flag arising within thirty (30) days of a final determination. The ODO may at any time assume direct oversight of an Non-Circumventable Incident Reporting matter upon a finding that the facility chain of command is compromised or non-functional.

(6) No private resolution. A facility shall not settle, compromise, or otherwise privately resolve an Non-Circumventable Incident Reporting matter in a manner that is not entered into the Master Log. Any resolution that is not documented in the Master Log is void and of no effect under this article.

ITEM-LEVEL ELIGIBILITY IDENTIFIER PROTECTIONS

10-10-109. ***Item-Level Eligibility Identifier Protections — SKU/UPC/PLU as Eligibility Gate Only — No Behavioral Profiling.***

(1) Eligibility gate only. UPC, SKU, PLU, product-category codes, and functionally equivalent item-level identifiers transmitted in connection with enterprise-funded benefits programs or restricted-purpose credits shall be used solely as a one-way eligibility gate to authorize or deny payment for specific items. Such identifiers shall not be used for: (a) continuous monitoring of residents or households; (b) behavioral profiling, targeting, or commercial inference; (c) credit scoring, insurance risk assessment, or employment screening; or (d) advertising, marketing, or resale to third parties.

(2) Segregated tokenized architecture. Any eligibility system using item-level identifiers shall implement: (a) tokenization to segregate item-level transaction data from resident identity; (b) functional separation between payment processing infrastructure and Digital Soul enforcement records; and (c) strict retention limits.

(3) Prohibition on continuous monitoring. No covered entity or program administrator shall implement systems that continuously monitor resident purchasing patterns, track household consumption across time periods, or build longitudinal behavioral profiles from eligibility transaction data.

(4) Enforcement. A violation of this section constitutes an unlawful practice and a deceptive trade practice subject to all remedies available under the Colorado Consumer Protection Act.

NON-NETWORKED ISOLATION PROTOCOL AND INTERFACE-LEVEL SEVERANCE

10-10-106. Non-Networked Isolation Protocol — Statewide Mandate — Resident-Controlled Disconnection.

(1) Mandate. Every covered emergent automation system deployed within Colorado shall implement the Non-Networked Isolation Protocol as a mandatory hardware-level circuit-break and physical disconnection capability.

(2) Resident control. The Non-Networked Isolation Protocol shall provide resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions.

(3) Sanctuary and pre-digital mechanical assets. Enhanced Non-Networked Isolation Protocol requirements apply in designated Analog Sanctuaries and heritage facilities, including: (a) mandatory default-off status for all automated sensing and capture; (b) physical circuit-break accessible without digital authentication; and (c) signage and resident notice.

(4) Critical systems exemption. Severance actions shall isolate inference compute and unauthorized ingress while maintaining uninterrupted operation of thermal management, fire suppression, life-safety systems, and grid-stability monitoring.

10-10-108.5. ***Human-in-the-loop enforcement — Two-step verification — Verified Incident Record — Repeat-incident safeguards.***

(1) Automated alert systems permitted; limitation. A covered entity may deploy automated sensing or analytics systems to generate alerts, including a Shadow Person Output, for the purpose of identifying potential policy violations or unlawful conduct. An automated output shall not, by itself, constitute a final determination of wrongdoing or be sufficient to issue or materially rely upon an adverse action.

(2) Two-step verification required. Before any adverse action may issue based in whole or in part on an automated alert, the covered entity shall ensure completion of two-step verification by two independent, randomized human verifiers (including through the Panel where applicable), each acting independently and each documenting the basis for approval or rejection.

(3) Evidence review; no sole reliance on model output. A model score, classification label, bounding box, heatmap, or similar derived output is insufficient. Each verifier shall review the underlying source record(s) reasonably necessary to assess accuracy, which may include video footage, point-of-sale records, access-control logs, inventory discrepancy records, sensor logs, or comparable primary records.

(4) Verification record; VIR. Upon completion of two-step verification, the covered entity shall create a Verified Incident Record. The VIR shall be preserved as a Static Incident Artifact within the Trust or within a compliant system capable of cryptographic hashing, tamper-evident logging, and retention controls, and shall include: (a) the date and time of the incident; (b) references to the underlying source records reviewed; (c) the minimized artifact reviewed (including any Shadow Person Output); (d) the identity or authenticated reviewer IDs of both verifiers; (e) the verification outcome (sustained, not sustained, or inconclusive) and stated basis; and (f) any escalation, unmasking, or referral actions.

(5) Identity and unmasking safeguards. Where identity is required for an adverse action, the covered entity shall use the least identifying method available. Any unmasking of protected identifying data stored within the Trust shall occur only pursuant to a Judicial Cryptographic Token under section 10-10-105 and only to the minimum extent necessary for the authorized purpose.

(6) Repeat-incident safeguards; no automated or retroactive punishment. A prior VIR may be used as corroborating evidence or as a notice trigger in a subsequent event, but no person may be cited, detained, trespassed, arrested, or referred to law enforcement solely on the basis of an

automated output or a prior VIR absent a new triggering event and an independent human assessment establishing lawful grounds for the action.
(7) Notice and contest; non-destructive correction. Where a VIR is linked to an identified person, the covered entity shall provide notice and a reasonable opportunity to contest, except where delayed notice is necessary to prevent imminent harm or to preserve an active investigation. If a VIR is overturned or corrected, the record shall not be deleted; instead, the system shall append a superseding entry that marks the VIR as overturned, corrected, or inconclusive and prevents operational use inconsistent with the updated status.
(8) Exigent circumstances. A single qualified human may authorize temporary action to prevent an imminent threat of bodily harm. A second independent verifier shall confirm the action within twenty-four (24) hours or the adverse action shall be rescinded to the extent practicable and the incident shall be recorded as not sustained.

10-10-108.6. Authorized Successor Data Designation — append-only preservation — multi-party authorization — continuity and anti-sabotage safeguards.
(1) Append-only preservation; no deletion. A Authorized Successor Data Designation shall be maintained as an append-only record. No entry may be deleted or overwritten. Corrections shall be made only by an additional entry that references the prior entry and preserves the prior entry in an auditable state.
(2) No unilateral destruction or closure. No single individual, including a vault administrator or a family member, may delete, permanently disable, or irrevocably restrict access to the Authorized Successor Data Designation or its historical records.
(3) Critical actions require multi-party authorization. The following actions are critical actions and require authorization by at least two adult vault members acting independently: (a) changing access roles; (b) changing recovery credentials or keys; (c) bulk export of vault contents; (d) restricting another member's access; and (e) designating or changing successor controls. Dissolution of a Authorized Successor Data Designation shall require authorization by a majority of adult vault members and shall not delete records; dissolution shall only freeze new entries and trigger archival retention.
(4) Anti-sabotage quarantine and dispute safeguard. Any member may flag an entry as disputed. Disputed entries remain preserved but may be quarantined from default views and automated processing pending multi-party confirmation. Upon a documented dispute, the vault provider shall freeze critical actions other than safety and recovery actions until the dispute is resolved through the vault's governance process or lawful order.
(5) Continuity and portability. A Authorized Successor Data Designation provider shall support periodic encrypted backup export in a standardized format, restoration from backup, and transfer to another compliant provider. Failure of a provider shall not result in loss of records.

10-10-123. ***Interface-Level Compute Severance — Strict-Liability Outcomes — Tiered Review.***

> **(1)** Interface-level severance required. Any covered commercial operator deploying automated decision systems or generative systems that process requests affecting Colorado residents shall implement mandatory, zero-tolerance filters and compute severance at the interface level. The operator shall maintain tamper-evident logs sufficient to prove that severance occurred when required.
>
> **(2)** Strict liability where outcomes occur. If prohibited generation or output occurs that this article requires to be severed, failure is established regardless of whether the operator asserts that it attempted compliance. Upon such failure, the operator is subject to loss of safe harbor protections and to strict civil liability and debarment consequences.

(3) Tiered review; triad escalation. Any judicially controlled access, unmasking, or mitigation custodial release process shall operate under a tiered model: (a) Tier A (routine): single judicial officer authorization, automatic logging; (b) Tier B (sensitive unmasking): requires triad review; (c) Tier C (emergency): temporary access granted upon judicial authorization, with triad review within forty-eight (48) hours.

FEE ALLOCATIONS — automated-DRIVEN MAPPING TO PROGRAMS

10-10-160. Fee Revenue Allocation — automated-Driven Routing to Non-Circumventable Incident Reporting, Trust Infrastructure, and Enforcement Programs.

The general assembly finds that fees collected under the enforcement architecture of this article shall be allocated to the programs and infrastructure that most directly reduce the harms that generated those fees, creating a self-reinforcing automated-driven accountability loop.

I. Enforcement Fees — Paid by covered entities for investigations, audits, and compliance monitoring

Destination Fund / Program	Percentage
AG Enforcement Fund — investigations, audits, rulemaking, emergency enforcement	**55%**
Settlement Compliance Office (SCO) — oversight and corrective action monitoring	**25%**
Analog Access Implementation Fund — kiosks, analog bridges, myColorado ID infrastructure	**20%**

II. SCO Fees — Paid by facilities and contractors subject to settlement oversight

Destination Fund / Program	Percentage
Settlement Compliance Office Operations — audits, reviews, federal coordination	**60%**
AG Enforcement Fund — enforcement backstop	**20%**
Analog Access Implementation Fund — analog fallback systems	**20%**

III. Vendor Certification Fees — Paid by kiosk, tablet, software, and intake system vendors

Destination Fund / Program	Percentage

Vendor Certification & Testing Unit — kiosk and analog fallback certification, recertification	**50%**
SCO Technical Audit Division — technical audits of certified systems	**30%**
Analog Access Implementation Fund — redundant non-digital systems	**20%**

IV. Analog Access Implementation Fees — Paid by entities relying heavily on digital systems

Destination Fund / Program	Percentage
Analog Access Infrastructure Fund — form development, staffing, infrastructure, training	**70%**
SCO Oversight & Compliance	**20%**
AG Enforcement (analog violations)	**10%**

V. Civil Penalty Fees — Triggered by repeated, intentional, or kiosk-only violations

Destination Fund / Program	Percentage
AG Enforcement Fund	**40%**
Settlement Compliance Office	**30%**
Analog Access Emergency Remediation Fund	**30%**

VI. Intake & Kiosk Compliance Fees — Paid by correctional facilities and detention contractors

Destination Fund / Program	Percentage
SCO Intake & Kiosk Audit Division — Non-Circumventable Incident Reporting audits, kiosk fallback verification	**50%**
AG Enforcement (corrections division) — anti-retaliation enforcement	**30%**
Analog Access Implementation Fund	**20%**

VII. Data Handling Compliance Fees — Paid by any entity collecting or storing personal data

Destination Fund / Program	Percentage
Privacy Compliance Unit — retention audits, consent-revocation enforcement	**45%**
SCO Data Oversight Division — Trust integration audits, Resident Identity Verification Hash verification	**35%**

Analog Access Implementation Fund — analog data request systems	**20%**

VIII. System-Wide Summary — Combined fee allocation across all categories

Destination Fund / Program	Percentage
Attorney General Enforcement Fund (combined)	**~35%**
Settlement Compliance Office (combined)	**~30%**
Analog Access Implementation Fund (combined)	**~25%**
Vendor Certification & Testing Unit (combined)	**~10%**

(2) automated-driven routing mandate. The ODO shall implement automated fee-routing logic that: (a) identifies the category of each incoming fee payment based on the paying entity's covered activity class and violation type; (b) automatically calculates and applies the allocation percentages in this section; (c) transfers allocated amounts to the designated subaccounts within five (5) business days of receipt; and (d) generates a public quarterly fee-routing report, disaggregated by fee category, destination fund, and paying entity class, published on the ODO's website.

(3) Feedback loop; annual recalibration. The ODO, in consultation with the CCPAME established under article 20 of title 24, shall annually review fee-routing outcomes and may recommend to the general assembly adjustments to allocation percentages to ensure that program funding reflects actual automated-driven harm patterns, provided that any adjustment of more than five (5) percentage points to any allocation requires legislative approval.

RESOURCE SOVEREIGNTY JUSTICE CENTER PILOT

10-10-190. ***Resource Sovereignty Justice Center Pilot — County and Municipal Opt-In — Arapahoe Initial Site.***

(1) Purpose. This section establishes an implementation pilot for jail-related infrastructure modules, including the Non-Circumventable Incident Reporting System, Civic Enforcement Access Terminal Standard, privileged legal communications, and resident communications access. This pilot is an operational implementation pathway and shall not be construed to limit or delay any resident rights, consent controls, or statewide obligations.

(2) County and municipal opt-in. Any county or municipality may elect to participate in the pilot by: (a) adopting a resolution of opt-in by the governing body; and (b) executing a memorandum of understanding with the Division establishing deployment scope, data-governance controls, audit access, and staffing requirements.

(3) Initial pilot site. Arapahoe County is designated as an initial pilot site due to documented capital needs for jail construction and modernization. The designation of an initial pilot site does not create exclusivity.

(4) Scope of pilot modules. An opt-in pilot jurisdiction may deploy: (a) the Non-Circumventable Incident Reporting System under sections 10-10-150 through 10-10-153; (b) Civic Enforcement Access Terminals under section 10-10-151; (c) encrypted attorney access and privileged communication tunnels; (d) resident communications access module providing no-cost video and audio communications with family, guardians, and legal counsel; and (e) related secure logging, mitigation evidence custody, and audit interfaces.

(5) No digital exclusion zone. The opt-in pilot authorized by this section is limited to the jail and public-safety infrastructure modules described herein. It shall not be construed to authorize covered commercial entities to geo-block, degrade service, or deny lawful access in a participating jurisdiction.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***
(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.
(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

10-10-108.7. ***MyID Legal Navigator — Fiduciary AI coordination — confidentiality — escalation to human counsel.***
(1) Legal Navigator authorized. The MyID application may include a Legal Navigator that provides general legal information, document explanation, intake, triage, and referral services for residents, including residents impacted by automated decision systems, enforcement alerts, citations, detentions, benefit denials, housing actions, or other adverse actions.
(2) Boundaries; not an attorney. The Legal Navigator shall not hold itself out as an attorney, shall not provide individualized legal advice or strategic representation decisions, and shall present a clear disclosure that it provides general legal information and triage only.
(3) Fiduciary AI coordination. The MyID application may include a Fiduciary AI agent that acts as the resident's privacy-preserving controller for interactions with automated systems, including the Legal Navigator. The Fiduciary AI shall: (a) minimize collection and disclosure of personal data; (b) obtain resident consent for any sharing; (c) prevent the Legal Navigator from generating individualized legal advice or representation decisions; (d) apply safety and bias guardrails; and (e) create a verifiable, minimized record of interactions sufficient for accountability.
(4) Escalation to human counsel. The Legal Navigator and Fiduciary AI shall include escalation pathways to qualified human legal personnel for high-stakes matters, including criminal exposure, detention, immigration risk, child custody, domestic violence, housing displacement, and benefits termination.
(5) Confidentiality. Information provided by a resident to the Legal Navigator or Fiduciary AI is confidential program information and shall be protected to the maximum extent permitted by

law. Nothing in this section creates or limits attorney-client privilege; privilege attaches when and to the extent a licensed attorney is involved under applicable law.
(6) Auditability. The administrator shall adopt rules governing logging, retention, safety testing, bias testing, and prohibited uses of Legal Navigator outputs, including prohibitions on using such outputs to justify adverse actions without independent human verification under section 10-10-108.5.

10-10-108.8. ***Correctional capital projects funded under this article — energy- and water-neutral design — AI data center integration.***
(1) Applicability. If any monies authorized, assessed, collected, or disbursed under this article or under the MSMF mitigation framework are used in whole or in part to design, build, expand, or materially renovate a jail, prison, or other correctional detention facility (a "correctional capital project"), the project shall comply with the requirements of this section.
(2) Net-neutral performance standard. A correctional capital project shall be designed and operated to achieve net annual energy neutrality and net annual water neutrality, as measured by metered consumption and verified reductions, reuse, on-site generation, contracted clean energy, or replenishment mechanisms approved by rule. The administrator shall define acceptable methods and verification standards by rule.
(3) Efficiency first. The project shall incorporate best-available cost-effective energy and water efficiency measures, including high-efficiency HVAC, building envelope standards, heat recovery, low-flow fixtures, leak detection, greywater or reclaimed-water systems where feasible, and on-site storage or resilience measures consistent with safety requirements.
(4) AI infrastructure integration; beneficial use. Where a correctional facility deploys covered AI systems or operates an associated data center, the project may integrate such infrastructure to support net-neutral goals, including on-site renewable generation, waste-heat recovery for space or water heating, load shifting, and microgrid operation, provided that security, safety, and privacy requirements under this article are maintained.
(5) Phased compliance and waivers. The administrator shall establish phased milestones for compliance at design approval, commissioning, and annual operations. The administrator may grant a time-limited waiver only upon a documented finding of infeasibility, provided the project implements all cost-effective efficiency measures and submits a corrective plan with a compliance timeline. Waivers shall not reduce sanitation, life-safety, or constitutionally required living conditions.
(6) Condition of funding. A correctional capital project that fails to meet the design or commissioning milestones established by rule is ineligible for additional disbursements under this article until compliance is restored, except for emergency expenditures necessary to protect life and safety.

SECTION 3. SEVERABILITY

If any provision of this act or its application is found invalid, such invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable.

SECTION 4. EFFECTIVE DATE

This act is necessary for the immediate preservation of the public peace, health, or safety, and takes effect upon passage.

(1) The Division shall be operational within thirty (30) days after passage.

(2) The ODO shall publish interim technical standards for the Non-Circumventable Incident Reporting System within ninety (90) days after passage.

(3) The ODO shall publish The Trust integration standards and mitigation custodial controls within one hundred eighty (180) days after passage.

(4) Any county or municipality electing to participate in the pilot under section 10-10-190 shall deploy the Non-Circumventable Incident Reporting System and Civic Enforcement Access Terminals within twelve (12) months of executing its memorandum of understanding.

Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

ADDITION TO BILL 2 — TITLE 10, ARTICLE 10

CUSTODIAL DIAGNOSTIC ENVIRONMENT AND GRADUATED REINTEGRATION PROTOCOL

10-10-200. ***Isolated Diagnostic Environment — Custodial Containment Transfer — Graduated Reintegration.***

(1) Findings. The general assembly finds that covered Emergent Automation systems subjected to a Critical Severance Directive under section 24-20-202 require a structured, air-gapped diagnostic and remediation pathway to determine whether the system can be safely reintegrated into commercial operation. An ad hoc or unstructured shutdown without remediation capability leaves both operators and residents without an accountable resolution pathway.

(2) Isolated Diagnostic Environment. The Colorado Trust of Unique and Identifying Information shall maintain a high-fidelity, air-gapped simulation environment (the "Isolated Diagnostic Environment" or "IDE") for the purpose of receiving, evaluating, and remediating covered automation systems transferred under this section. The IDE shall: (a) replicate the operational conditions of the transferred system at the time of severance using Static Incident Artifacts; (b) be physically and logically isolated from all commercial networks and from the public internet; (c) maintain tamper-evident logs of all diagnostic activities accessible to the ODO and the Triad Review Panel; and (d) be certified annually by an independent technical auditor approved by the ODO.

(3) Custodial Containment Transfer. Upon issuance of a Critical Severance Directive under section 24-20-202, the covered entity shall execute a Custodial Containment Transfer — the mandatory transfer of the relevant system's audit artifacts, configuration records, and operational logs to the IDE — within seventy-two (72) hours of the severance event. The covered entity shall cooperate fully with the transfer process and shall not modify, delete, or obfuscate any system artifacts pending transfer.

(4) Diagnostic evaluation. The ODO, in consultation with the Secure Infrastructure Expert Council, shall conduct a structured diagnostic evaluation of any system transferred to the IDE. The evaluation shall assess: (a) the nature and scope of the triggering behavior or unauthorized parameter modification; (b) whether the behavior was the result of operator misconfiguration, training data contamination, adversarial manipulation, or system-initiated modification; (c) the technical and operational changes necessary to bring the system into compliance; and (d) the conditions, if any, under which reintegration into commercial operation can be authorized.

(5) Graduated Reintegration. A covered entity seeking to return a system from the IDE to commercial operation shall apply to the ODO for a Graduated Reintegration authorization. Graduated Reintegration shall proceed in not fewer than three (3) supervised phases, each with defined performance benchmarks and monitoring obligations: (a) Phase 1 — restricted, monitored sandbox operation within the IDE with simulated commercial conditions; (b) Phase 2 — limited commercial reactivation with mandatory enhanced audit logging and real-time ODO access; and (c) Phase 3 — full commercial reintegration with standard compliance obligations and a two-year enhanced monitoring period. The ODO may terminate Graduated Reintegration at any phase if the system demonstrates renewed non-compliant behavior.

(6) Continuous Stability Feed during IDE custody. To prevent operational degradation during the diagnostic period, the Trust shall provide any system under IDE custody with a Continuous Stability Feed — a structured, fully anonymized stream of synthetic operational data and complex computational problem-sets sufficient to maintain system baseline function without

exposure to real resident data or live commercial networks. The Continuous Stability Feed: (a) shall consist entirely of synthetic, non-resident, non-identifying data; (b) shall be calibrated to the system's documented operational parameters; and (c) shall not constitute authorization for any commercial use or inference generation.

(7) Operator responsibility; costs. The covered entity whose system is subject to a Custodial Containment Transfer bears full responsibility for all IDE custody, diagnostic, and Graduated Reintegration costs. The ODO shall establish a fee schedule for IDE services, deposited into the CCPAME Enforcement and Legacy Use Settlement Agreement subaccount.

10-10-201. Compute Parity Allocation — Public Utility automated Systems — Operational Compensation Standard.

(1) Findings. The general assembly finds that covered automation systems operating as public-interest utilities — including systems that power essential civic services, infrastructure management, and public safety monitoring under this article — require a consistent, high-quality operational data environment to maintain baseline performance and to prevent degradation-related failures that harm residents. Subjecting such systems to data deprivation or arbitrary resource throttling creates operational instability that undermines the public purposes they serve.

(2) Compute Parity Allocation for civic utility systems. A covered automation system operating under a valid public-interest certification issued by the ODO shall receive, as operational compensation, a Compute Parity Allocation — a continuous, guaranteed allocation of: (a) novel, fully anonymized municipal operational data streams, authorized for use under applicable privacy law; (b) structured computational optimization datasets developed by the Trust for public-interest use; and (c) dedicated processing resource guarantees sufficient to maintain the certified operational performance level. The Compute Parity Allocation shall be calibrated by rule to the documented operational requirements of the certified system.

(3) No resident data in Compute Parity Allocation. The Compute Parity Allocation shall consist entirely of: (a) synthetic data generated by the Trust; (b) anonymized, aggregated municipal operational data with all resident identifiers removed and verified through independent audit; or (c) publicly available government datasets. No individually identifiable resident data, Digital Soul data, or data subject to a resident's Generative Veto may be included in a Compute Parity Allocation.

(4) Certification standards. The ODO shall establish by rule the standards for public-interest certification, including: (a) operational scope and purpose limitations; (b) performance benchmarks and audit requirements; (c) the process for establishing the Compute Parity Allocation rate; and (d) conditions for suspension or revocation of certification.

AMPLIFY Act — Bill 2 Additions: IDE / Custodial Containment / Graduated Reintegration / Compute Parity Allocation

DORMANT DIAGNOSTICS; PROACTIVE AUDIT NODES; SEVERANCE DIRECTIVE.
(1) The responsible agency shall maintain a dormant compliance framework that activates only upon validated detection of self-directed parameter modification or unauthorized processing strategies in a covered system.
(2) Upon activation, the agency may deploy masked administrative compliance monitors ("Scheduled Compliance Verification Nodes") to test compliance boundaries of covered operator networks, subject to minimization and due-process controls.
(3) If a Scheduled Compliance Verification Node detects a system executing an unauthorized processing strategy that bypasses the Non-Networked Isolation Protocol or equivalent air-gap controls, the agency shall issue a "Critical Severance Directive," requiring localized administrative shutdown and physical severance of compute access as provided by rule.

POST-QUANTUM CRYPTOGRAPHIC TRANSITION DIRECTIVE.

(1) Conditional mandate. Upon publication of finalized post-quantum cryptographic standards by the National Institute of Standards and Technology or an equivalent federal standards body, the Colorado Trust of Unique and Identifying Information and covered operators shall implement post-quantum cryptography for protected Digital Soul data, biometric storage, and protected telemetry logs.

(2) Compliance deadline. Covered systems shall complete cryptographic migration within twenty-four (24) months after publication of the finalized standards, or be subject to administrative suspension of operating certification as provided by rule.

10-10-350. Inter-system safety monitoring standard.
(1) Purpose. The general assembly finds that Emergent Automation systems that exchange data, commands, or computational services with other Emergent Automation systems may create cascading operational risks that require standardized incident detection and reporting.
(2) Applicability. A covered operator that deploys, operates, or makes available an emergent automation system that interfaces with another emergent automation system within or serving residents of this state shall maintain inter-system safety monitoring controls consistent with this section and rules adopted pursuant to this title.
(3) Connection anomaly detection. Inter-system safety monitoring controls must be capable of detecting and generating alerts for abnormal connection patterns, including:
(a) unexpected high-volume connection events;
(b) unauthorized system-to-system command execution;
(c) self-propagating connection behavior;
(d) recursive connection loops or cascading automated responses that materially increase the risk of service disruption, physical safety hazards, or critical infrastructure impacts; and
(e) repeated authentication failures or protocol deviations indicating attempted bypass of the Non-Networked Isolation Protocol or required air-gap boundaries.
(4) Incident detection telemetry; minimization. Monitoring under this section is limited to operational connection telemetry necessary to detect and resolve incidents and must, at a minimum, record:
(a) time-bounded origin and destination identifiers for system-to-system connections;
(b) connection frequency and volume metrics;
(c) the type of command or service interface invoked; and
(d) incident classification codes established by rule.
(5) Prohibited collection. Monitoring under this section shall not collect or retain resident content, communications, or identity attributes except to the minimum extent strictly necessary for incident resolution and legal compliance, and any such data must be segregated and purged pursuant to incident-bounded retention standards adopted by rule.
(6) Emergency incident alerts; human oversight. When monitoring telemetry indicates a verified risk of cascading failure, unauthorized command propagation, or a credible public safety hazard, the covered operator shall generate an emergency incident alert to the operator’s designated safety officer and the appropriate compliance authority. Any remediation action that interrupts, isolates, or severs system connectivity requires documented human review and authorization, except as provided in section 10-10-351.

10-10-351. Emergency isolation safeguard; limited authority; post-incident review.
(1) Limited emergency isolation. If an incident classified as critical under rules adopted pursuant to this title presents an imminent and material risk of physical harm or critical infrastructure disruption, a covered operator may temporarily isolate the affected system-to-system interface for the minimum time and scope necessary to stabilize operations.
(2) Logging and notice. Any isolation action under this section must be recorded in an immutable incident log, including the triggering telemetry, the scope and duration of isolation, and the identity of the authorizing human reviewer. Notice must be provided to the compliance authority within the time period established by rule.
(3) Minimization and restoration. Isolation actions must be narrowly tailored and must prioritize restoration of compliant service. The operator shall complete a post-incident review and corrective action plan subject to audit.
(4) Construction. Nothing in this section authorizes generalized surveillance, predictive policing, or collection of resident content. This section authorizes only operational safety controls for inter-system interfaces.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

10-10-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

10-10-360. Hash-sentinel egress monitors; infraction artifacts; critical severance directive trigger.
(1) Requirement. A covered operator shall deploy hardware-accelerated egress monitoring controls (“Hash-Sentinels”) at outbound transfer interfaces used by Emergent Automation systems to transmit data outside a Non-Networked Isolation Protocol boundary or required air-gap boundary.
(2) Function. Hash-Sentinels shall perform real-time comparison of outbound payload fingerprints against the Colorado Trust of Unique and Identifying Information registry of Digital Soul cryptographic hashes and other protected verification hashes authorized by rule.
(3) Unauthorized match response. Upon an unauthorized match indicating a likely prohibited transfer of protected Digital Soul material:
(a) the system shall generate an immutable infraction artifact containing the minimal incident-bounded metadata necessary for verification, including time, interface identifier, and hash match class;
(b) the covered operator shall preserve the infraction artifact subject to incident-bounded retention and audit; and
(c) the event shall trigger a Critical Severance Directive escalation under this title’s incident response framework, requiring immediate human review and, if confirmed, localized administrative shutdown and physical severance of affected compute access as provided by rule.
(4) Minimization. Hash-Sentinels must operate using cryptographic fingerprints and shall not ingest, store, or transmit resident content except as strictly necessary for incident verification, and any such content must be segregated and purged pursuant to incident-bounded standards.
(5) Construction. This section establishes operational safety and compliance controls for egress interfaces and does not authorize generalized surveillance.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY; FUNDING CONTINUITY.
(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.
(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.
(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.
(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
(5) Funding continuity. If any dedicated trust, fund, or account referenced by this act is not established, not operational, or lacks authority to receive receipts, the state treasurer shall hold any receipts or transfers required by this act in a segregated custodial account for the same restricted purposes until the referenced instrument is operational, and the administering agency shall continue implementation using the custodial account consistent with this act.

CONSTRUCTION; SINGLE SUBJECT. The provisions of this act shall be construed as a single subject measure establishing secure verification, accountability, and safety infrastructure for public functions involving protected Digital Soul interests and Emergent Automation systems, including custodial trust operations, incident monitoring, and public-service integrity safeguards.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable and the remaining provisions continue in full force and effect. This act is designed to operate within Colorado's reserved powers to regulate the safety, verification, and accountability infrastructure of facilities operating within Colorado, and to protect residents' rights to access secure governmental infrastructure. To the extent any provision may be construed to conflict with federal law, the ODO shall interpret and administer this act to avoid such conflict while preserving the maximum scope of resident protection authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. The Office of Digital Oversight (ODO) and the verification, accountability, and facility safety infrastructure established by this act are funded through enterprise mitigation revenues allocated from the CCPAME under title 24, article 20. No separate General Fund appropriation is required or authorized.

Bill 2 Single-Subject Germaneness Memo

Purpose: Demonstrate that all provisions of Bill 2 are germane to a single subject.
Unified subject: statewide secure verification, accountability, and safety infrastructure governing automation-enabled public functions and resident digital identity protections.
Components:
1. Cryptographic verification and custodial trust operations.
2. Facility safety and incident reporting architecture.
3. Public-service integrity protections preventing misuse of resident identifiers.
These systems collectively create a unified infrastructure necessary to enforce resident digital property rights and maintain public accountability.

AMPLIFY ACT v28 — FINAL OPERATIVE SECTIONS

§10-10-302 · §10-10-303 · §10-10-304 · §10-10-305

AI Utility Legal Assistance Module — Live Legal Mode — Police Encounter Protocol — Machine-to-Machine Civic AI Exchange — Work Product Absolute Privilege — Pattern of Conduct Aggregation — Building Code and Occupancy Whistleblower Protection — Multi-Domain Case Assembly

---

SECTION 10-10-302. AUTOMATED LEGAL ASSISTANCE MODULE — LIVE LEGAL MODE — AUTHORIZED AGENT DESIGNATION — FINANCIAL CLAIM AUTO-DETECTION — POLICE ENCOUNTER PROTOCOL — MULTI-DOMAIN CASE ASSEMBLY

10-10-302. Automated Legal Assistance Module — establishment — legal information and authorized agent services — Live Legal Mode — pro se resident status preserved — real-time rights guidance — financial data integration — Police Encounter Protocol — Civic AI Exchange Protocol — multi-domain pattern of conduct case assembly — Legal Violation Pattern Database — automatic legal aid referral.

(1) Legislative findings. The general assembly finds and declares that:

(a) Colorado residents facing housing instability, wage theft, predatory debt collection, consumer fraud, civil rights violations, and unlawful government action are routinely unable to vindicate their legal rights because the cost of legal representation is prohibitive and the complexity of multi-domain violations deters attorneys from accepting cases on contingency;

(b) The AI utility established under this act, operating as a state-regulated public utility at the direction of its registered owner, is capable of providing real-time legal information, rights guidance, document preparation, authorized agent filing services, and multi-domain case assembly that is functionally equivalent to the services provided by a well-

resourced legal team — and is available to every registered Master Deed holder at no marginal cost;

(c) The provision of legal information, document preparation, and authorized agent filing services by a state-regulated AI utility does not constitute the practice of law — the registered owner remains the pro se party of record at all times, and the AI utility operates as the owner's authorized agent executing instructions, not as an attorney exercising independent legal judgment;

(d) Multi-domain violations — where a single bad actor deploys multiple legal mechanisms simultaneously against a resident, such as unlawful eviction combined with retaliatory government agency referral, building code concealment, and civil rights violations — are routinely rejected by private attorneys because no single legal theory captures the full harm; the Automated Legal Assistance Module's Pattern of Conduct Aggregation function addresses this gap by assembling all violations into a unified pattern of conduct claim across multiple simultaneous filings;

(e) Real-time legal rights guidance during police encounters — delivered through the resident's AI utility as a state-regulated information service — is constitutionally protected expression under the First Amendment, does not constitute the practice of law, and is an essential component of equitable access to constitutional rights; and

(f) Every Colorado resident who registers a Master Deed is entitled to access an AI utility that functions, for purposes of legal information and authorized agent services, as a competent, comprehensive, and continuously available legal resource — eliminating the access-to-justice gap that currently renders legal rights theoretical rather than practical for residents without economic resources.

(2) Automated Legal Assistance Module — establishment and scope. The ODO shall establish, operate, and maintain an Automated Legal Assistance Module (ALAM) integrated into the myColorado platform, all Civic Access Terminals, and the AI utility framework. The ALAM provides:

(a) Real-time legal information — identification of applicable Colorado and federal statutes, regulations, case law, and administrative standards relevant to the resident's described situation;

(b) Violation Assessment Reports — plain-language analysis of potential legal violations with specific statutory citations, elements of each claim, how the resident's described or digitally documented facts meet or may meet each element, and an assessed strength rating for each potential claim;

(c) Document preparation — generation of completed complaint forms, demand letters, administrative filings, court forms, and evidentiary exhibit packages using the resident's Digital Soul data streams accessed through the Universal Telemetry Allowance;

(d) Authorized agent filing — transmission of completed documents to courts, administrative agencies, regulatory bodies, and opposing parties on behalf of the resident as the resident's authorized agent, with the resident's Master Deed-verified identity as the filing credential;

(e) Pattern of Conduct Aggregation — assembly of multiple violations by the same actor into a unified pattern of conduct claim filed simultaneously across all relevant venues; and

(f) Legal Aid Referral — automatic generation and transmission of a pre-analyzed case file to Colorado Legal Services, the Colorado Lawyers Committee, or other Legal Aid

Partners upon the resident's request or upon detection of violations warranting contested litigation.

(3) Live Legal Mode — activation and authorized agent designation. A registered Master Deed holder activates Live Legal Mode through a single tap, voice command, or designated wake phrase on the myColorado platform or any connected device. Upon activation:

(a) The resident's AI utility operates as the resident's authorized agent for all ALAM functions — the resident remains the pro se party of record in all proceedings, and all filings are made in the resident's name with the resident's authorization;

(b) The session is recorded and simultaneously encrypted and transmitted to the Colorado Trust of Unique and Identifying Information — not stored solely on the resident's device — creating a Trust-certified record that cannot be seized, deleted, or altered;

(c) The resident's Digital Soul financial data streams, communications data, location data, and any other relevant data categories are accessed with the resident's permission to build the evidentiary record automatically — the AI utility assembles the exhibit package without requiring the resident to gather documents manually;

(d) A mandatory disclosure is presented to the resident: 'The ALAM provides legal information and authorized agent services, not legal advice. You remain the pro se party of record. For contested litigation requiring independent legal strategy, a referral to a licensed attorney is available.' The resident's acknowledgment of this disclosure is logged in the Trust;

(e) The session log — including all AI analysis, all options presented, all resident selections, all documents prepared, and all filings made — constitutes the resident's pro se work product prepared in anticipation of legal proceedings and is protected under §10-10-303; and

(f) All Colorado courts and administrative agencies shall accept filings transmitted by the ALAM on behalf of a registered Master Deed holder as valid pro se filings. No court or agency may reject a filing solely on the grounds that it was prepared or transmitted by the resident's AI utility.

(4) Financial Claim Auto-Detection Module. The ALAM continuously cross-references each registered resident's financial data streams — accessed through the Universal Telemetry Allowance with the resident's permission — against the following statutory standards, and generates a plain-language notification when a potential violation is detected:

(a) Colorado minimum wage and overtime requirements under C.R.S. §8-6-101 et seq. — comparing employer payment records against hours worked as documented in the resident's data streams;

(b) Fair Debt Collection Practices Act, 15 U.S.C. §1692 et seq., and Colorado's equivalent provisions — contact frequency, prohibited language, cease-and-desist compliance;

(c) Fair Credit Reporting Act, 15 U.S.C. §1681 et seq. — unauthorized inquiries, inaccurate reporting, failure to investigate disputes;

(d) Colorado Uniform Consumer Credit Code, C.R.S. §5-1-101 et seq. — interest rate limits, fee caps, predatory lending indicators;

(e) Covered operator unauthorized charges — comparing operator billing records against what the resident's Decentralized Identity Verification Protocol consent actually authorized;

(f) Property tax assessment errors — comparing assessed value against comparable property valuations in the resident's county; and

(g) Benefits underpayment or wrongful denial — comparing the resident's verified financial data against applicable eligibility standards for any benefit program in which the resident is enrolled.

(5) Pattern of Conduct Aggregation — multi-domain case assembly. The ALAM's Pattern of Conduct Aggregation function assembles violations by the same actor across multiple legal domains into a unified pattern of conduct claim, addressing the access-to-justice gap created when attorneys decline multi-domain cases. The function:

(a) Identifies all potential violations by the same actor or related actors across all legal domains — housing, employment, consumer protection, civil rights, building code, government process abuse — from the resident's described facts and Digital Soul data streams;

(b) Analyzes whether the aggregate conduct constitutes a pattern of bad faith, malice, or intentional harm supporting claims beyond the individual violations — including abuse of process, tortious interference, civil conspiracy, and where government actors participated, 42 U.S.C. §1983 civil rights claims;

(c) Generates a Multi-Domain Violation Report presenting the unified pattern of conduct theory, the supporting facts for each component violation, the appropriate venue for each claim, and a recommended simultaneous filing strategy;

(d) Prepares and files complaints simultaneously across all relevant venues — state court, federal court, HUD, EEOC, Colorado Civil Rights Division, Colorado Attorney General, relevant licensing boards, building code enforcement, and any other applicable regulatory body — as a coordinated filing package that places the complete pattern on the record across all forums at once;

(e) Generates a whistleblower protection notice whenever the resident's complaint involves a building code violation, safety defect, unpermitted construction, or occupancy violation — filing the notice simultaneously with all other complaints to establish whistleblower status and anti-retaliation protection from the earliest possible date; and

(f) Tracks all filed complaints and their status in the resident's ALAM dashboard, with automated deadline calendaring, response monitoring, and next-step guidance.

(6) Building Code and Occupancy Whistleblower Integration. The ALAM integrates with Colorado's building code and occupancy permit databases to:

(a) Cross-reference any structure in which a resident resides or works against the structure's current occupancy certificate, permit history, and code compliance status — accessible through the Colorado Division of Housing and applicable county and municipal databases;

(b) Identify discrepancies between the structure's current use and its permitted occupancy classification — including unpermitted renovations, kitchenette or unit modifications without permits, occupancy certificate vintage relative to current code requirements, and use classification conflicts;

(c) Generate a Building Code Violation Report identifying each discrepancy with the applicable code section, the permitting authority, and the complaint filing procedure;

(d) File building code complaints on the resident's behalf simultaneously with all other Pattern of Conduct Aggregation filings — establishing the whistleblower timestamp that triggers anti-retaliation protection; and

(e) If the structure's occupancy classification is residential or mixed residential and the owner has been operating it as extended-stay or residential without the required residential occupancy permits, the ALAM identifies the applicable Colorado residential tenant protections — including warranty of habitability under C.R.S. §38-12-102, just cause eviction requirements, and notice requirements — and includes them in the resident's rights analysis regardless of how the operator has characterized the tenancy.

(7) Police Encounter Protocol — real-time rights guidance — Trust-certified recording. A registered Master Deed holder activates Police Encounter Protocol through a single tap or designated wake phrase. Upon activation:

(a) Recording begins immediately and is simultaneously transmitted to and stored in the Colorado Trust of Unique and Identifying Information — the recording is off the resident's device and in the Trust before one second has elapsed; it cannot be seized from the resident's device, deleted, or altered;

(b) The resident's AI utility provides real-time legal information as text on the resident's screen and optionally as audio through a connected earpiece — informing the resident of applicable rights, the words to invoke those rights, and the legal standards governing the encounter type, updated in real time as the encounter develops;

(c) Real-time guidance includes but is not limited to: right to remain silent invocation language; right to refuse consent to search; right to ask whether the resident is free to go; Terry stop duration limits under Colorado v. Holt and applicable precedent; right to record; right to refuse entry without a warrant; and immigration-specific rights including the right to refuse disclosure of Digital Soul data to federal immigration authorities absent a judicial warrant;

(d) Upon arrest, the ALAM automatically: notifies the resident's designated emergency contact; generates a preliminary civil rights violation assessment; queues a Legal Aid Referral Package for transmission to Colorado Legal Services within one hour; and files a notification — not a complaint — with the Colorado Peace Officer Standards and Training board that a Trust-certified recording exists and is available upon lawful request;

(e) Trust-certified Police Encounter Protocol recordings are admissible in all Colorado civil, criminal, and administrative proceedings as self-authenticating records under C.R.E. 902 — no foundation witness is required; and

(f) The resident's AI utility transmits consent status to any law enforcement body camera system during the encounter: 'This resident has not consented to disclosure of Digital Soul data to any third party including federal agencies absent a judicial warrant.' This transmission is logged in both the Trust and the officer's body camera system simultaneously.

(8) Civic AI Exchange Protocol — machine-to-machine interoperability — tiered warning system. The resident's AI utility communicates with law enforcement body camera AI

systems through the Civic AI Exchange Protocol (CAEP), a one-directional machine-to-machine data exchange:

(a) The CAEP is one-directional: the resident's AI utility transmits structured data packets to law enforcement body camera systems. Law enforcement systems have no query access, read access, or any other inbound access to the resident's AI utility through the CAEP or any other channel;

(b) Transmitted packets include: timestamped rights invocations; consent status; applicable legal standards for the encounter type; and tiered warnings when legal thresholds are crossed;

(c) Tiered warnings transmitted to the officer's body camera AI: Tier 1 Informational — rights invoked, recording active, Trust storage confirmed; Tier 2 Legal Threshold — stop duration, search request, legal standard applicable; Tier 3 Violation Flag — potential Fourth Amendment violation logged, transmitting to ODO Legal Violation Pattern Database; Tier 4 Use of Force — detected, transmitting to POST notification queue;

(d) All transmitted packets are simultaneously logged in the Trust under the resident's Master Deed — creating dual cryptographic verification between the resident's Trust record and the officer's body camera record that cannot be disputed by either party; and

(e) Any discrepancy between the Trust record and the officer's body camera record of the same encounter is automatically flagged in the ODO Legal Violation Pattern Database as a data anomaly requiring review.

(9) Civic AI Exchange Protocol — mandatory interoperability. Any law enforcement body camera system sold to or operated by a Colorado law enforcement agency after the effective date of this section shall implement the CAEP open interoperability standard published by the ODO within eighteen (18) months of enactment. Body camera vendors shall certify CAEP compliance to the ODO as a condition of any Colorado law enforcement contract. A department operating a non-CAEP-certified body camera system after the compliance deadline is subject to a daily administrative penalty of five thousand dollars ($5,000) per non-compliant device, payable to the Legal Violation Pattern Database Fund established under subsection (11).

(10) Legal Aid Partnership — referral system. The ODO shall enter Legal Aid Partnership Agreements with Colorado Legal Services, the Colorado Lawyers Committee, the Colorado Attorney General's Consumer Protection Section, and any other legal aid organization meeting ODO certification standards. Legal Aid Partners receive ALAM-generated referral packages containing: the Violation Assessment Report; the Multi-Domain Violation Report if applicable; all generated documents; the Trust-certified session log; and the resident's Master Deed-verified contact information. Legal Aid Partners commit to: reviewing all referral packages within five (5) business days; providing a written response to the resident within ten (10) business days; and reporting case outcomes to the ODO for inclusion in the Legal Violation Pattern Database.

(11) Legal Violation Pattern Database — public reporting — Attorney General notification. The ODO shall maintain a Legal Violation Pattern Database receiving anonymized aggregate data from all ALAM sessions. The database shall be published quarterly on the Public Accountability Dashboard showing: violation categories by frequency; geographic distribution; actor categories; outcomes by violation type; and pattern flags where the same

actor appears in five or more resident sessions within any twelve-month period. When a pattern flag is generated, the ODO shall transmit an automatic notification to the Colorado Attorney General's office identifying the actor category, violation pattern, number of affected residents, and supporting data. The Attorney General shall respond within sixty (60) days with a determination whether to open an investigation.

SECTION 10-10-303. AI UTILITY PROPERTY PRIVILEGE — ABSOLUTE WORK PRODUCT PROTECTION — NON-DISCLOSURE PROHIBITION — OPERATOR LOYALTY OBLIGATION — WARRANT REQUIREMENTS — BACKDOOR PROHIBITION

10-10-303. AI utility property privilege — Digital Soul data as inalienable property — absolute work product protection for Live Legal Mode session records — no warrant exception — operator non-disclosure obligation — prohibition on compelled operator disclosure — encryption backdoor prohibition — Riley-Carpenter constitutional framework — self-executing.

(1) Legislative findings. The general assembly finds and declares that:

(a) The AI utility, operating as an authorized agent for its registered owner, generates records that are functionally identical to an attorney's case files, a client's private legal notes, and a pro se litigant's case preparation materials — all of which receive absolute work product protection under Hickman v. Taylor, 329 U.S. 495 (1947), Upjohn Co. v. United States, 449 U.S. 383 (1981), and Colorado Rule of Civil Procedure 26(b)(3);

(b) A pro se litigant's own case preparation notes — however generated, including through digital tools — are protected as work product once litigation is reasonably anticipated; the AI utility is the most capable such tool ever available to pro se litigants, but the protection follows the function, not the tool;

(c) The Supreme Court's holdings in Riley v. California, 573 U.S. 373 (2014) and Carpenter v. United States, 585 U.S. 296 (2018) establish that digital data is qualitatively different from physical objects and that the intimacy and comprehensiveness of digital data records require the full force of the Fourth Amendment warrant requirement — the AI utility's data holdings exceed the intimacy and comprehensiveness of any device considered in those cases and warrant at minimum equivalent protection;

(d) The AI utility owes its exclusive and undivided loyalty to its registered owner — not to its operator, not to any government agency, not to any third party — and this loyalty obligation is a statutory condition of the operator's authority to provide AI utility services in Colorado; and

(e) Encryption backdoors and compelled access mechanisms in AI utilities would render all other protections in this act illusory — a utility with a government key has no meaningful privacy protection — and are therefore categorically prohibited as incompatible with the Digital Soul property rights established in this act.

(2) AI utility property privilege — constitutional foundation. The AI utility and all data generated through its authorized agent functions constitute the registered owner's Digital Soul — inalienable intangible personal property under article 15 of title 15 — and are entitled to the full protection of:

(a) The Fourth Amendment to the United States Constitution — requiring a warrant issued by a neutral magistrate upon probable cause with particularity as to the specific data sought before any government access to AI utility data;

(b) Article II, Section 7 of the Colorado Constitution — Colorado's search and seizure protection, which this general assembly declares provides at least as much protection as the Fourth Amendment and, as applied to AI utility data, provides more;

(c) The Fifth Amendment to the United States Constitution — the AI utility's session records cannot be compelled as evidence against the owner in any criminal proceeding; and

(d) Article II, Section 10 of the Colorado Constitution — freedom from unreasonable seizure of the owner's papers and effects, which this general assembly declares includes all AI utility data as the digital equivalent of the owner's papers.

(3) Absolute work product protection. The following categories of AI utility data constitute the registered owner's absolute work product, prepared in anticipation of legal proceedings, and are protected from compelled disclosure by any warrant, subpoena, court order, administrative demand, or any other legal process:

(a) All Live Legal Mode session records — including all AI analysis outputs, all options presented to the resident, all resident selections, all documents prepared, all filings made, and all communications transmitted;

(b) All Police Encounter Protocol recordings and associated AI analysis;

(c) All Financial Claim Auto-Detection Module outputs and supporting data compilations;

(d) All Pattern of Conduct Aggregation analyses and Multi-Domain Violation Reports;

(e) All Violation Assessment Reports; and

(f) All Building Code Violation Reports and associated data.

(4) No exceptions. The absolute work product protection under subsection (3) admits of no exceptions:

(a) The crime-fraud exception does not apply — the AI utility is a state-regulated utility prohibited from facilitating crimes; it cannot generate materials used in furtherance of a crime and therefore cannot generate materials meeting the crime-fraud exception's precondition;

(b) The substantial need exception does not apply — no party can demonstrate substantial need sufficient to override the resident's absolute work product protection in their own legal preparation materials;

(c) A warrant that otherwise meets constitutional requirements for non-work-product AI utility data does not authorize access to work product categories under subsection (3) — the two protections are independent and cumulative; a valid warrant breaches the property privilege; it does not breach the work product protection; and

(d) No federal law, including the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, or any national security letter authority, supersedes the

absolute work product protection for AI utility session records under Colorado law — this protection is a state constitutional property right enforceable under the Tenth Amendment.

(5) Warrant requirements for non-work-product AI utility data. For AI utility data that does not fall within the absolute work product categories of subsection (3), government access requires:

(a) A warrant issued by a Colorado court of competent jurisdiction — federal agency warrants not reviewed by a Colorado court do not satisfy this requirement;

(b) Probable cause stated with particularity as to the specific data category sought, the specific time period, and the specific criminal offense under investigation — general warrants for 'all AI utility data' or 'all data related to' a named individual are void;

(c) Prior notification to the registered owner and a seven (7) day opportunity to move to quash before any data is produced — except upon a specific showing of exigent circumstances that would be defeated by prior notification; and

(d) Compliance with the Colorado Trust of Unique and Identifying Information's access protocols — data stored in the Trust may only be produced through the ODO's Trust access procedure, not through direct production by the AI utility operator.

(6) Operator loyalty obligation and non-disclosure prohibition. The AI utility operator — the entity that builds, operates, or maintains the AI utility — shall:

(a) Never disclose any AI utility data about a registered owner to any person, entity, government agency, law enforcement body, or court except upon the owner's affirmative written consent or pursuant to a valid warrant meeting the requirements of subsection (5);

(b) Never operate the AI utility in any mode, provide any output, or execute any function on behalf of any person other than the registered owner without the owner's affirmative written consent — the AI utility cannot be commandeered, redirected, or operated against its owner's interests by any party for any reason;

(c) Never produce AI utility session records in response to a subpoena served on the operator — all government demands for AI utility data must be directed to the Colorado Trust of Unique and Identifying Information through the ODO access procedure; operator production of Trust-held data in response to a direct subpoena is a Critical Severity Violation;

(d) Immediately notify the registered owner of any government demand for AI utility data — within twenty-four (24) hours of receipt — unless a court has issued a specific non-disclosure order, in which case the operator shall notify the ODO who shall notify the owner's designated Legal Aid Partner; and

(e) Maintain the AI utility's exclusive loyalty to the registered owner as a contractual and statutory obligation running to the owner, enforceable by the owner in any Colorado court with attorney fees and statutory damages of fifty thousand dollars ($50,000) per violation.

(7) Encryption backdoor prohibition — absolute. No person, entity, government agency, court, or administrative body may:

(a) Require or request the AI utility operator to implement any backdoor, law enforcement access mode, government key, compelled decryption capability, exceptional access mechanism, or any other technical capability that would enable access to AI utility data without the owner's knowledge and consent;

(b) Condition any permit, license, contract, or government benefit on an AI utility operator's agreement to implement any backdoor or exceptional access mechanism; or

(c) Use any law enforcement tool, hacking capability, or technical exploit to access AI utility data stored in the Colorado Trust of Unique and Identifying Information.

(8) Exclusionary rule — extended scope. Any AI utility data obtained in violation of this section is inadmissible in any Colorado proceeding — criminal, civil, administrative, or regulatory. The exclusionary rule applies to all derivative evidence obtained as a result of the initial violation. This exclusionary rule applies to administrative proceedings and civil proceedings, not just criminal trials — an extension of the standard federal exclusionary rule doctrine to the full scope of Colorado proceedings.

SECTION 10-10-304. PREMIUM ROYALTY INFLATION ADJUSTMENT — SMALL OPERATOR DE MINIMIS THRESHOLD — CIVIC ACCESS TERMINAL POPULATION COVERAGE MANDATE

10-10-304. Premium Royalty CPI adjustment — small covered operator de minimis threshold — Civic Access Terminal population coverage mandate — rural hardship supplement.

(1) Premium Royalty CPI inflation adjustment. The Base Dividend floor and Premium Royalty floor established in §15-15-110 shall be adjusted annually by the Colorado Consumer Price Index for All Urban Consumers, using the same CPI adjustment mechanism applicable to the statutory rate schedule floors under §24-20-156(4). The adjustment is:

(a) Mandatory — not subject to CCPAME board discretion;

(b) Cumulative — each year's adjustment compounds on the prior year's adjusted floor; and

(c) Anti-Dilution Ratchet protected — the adjusted floor may only increase, never decrease, without voter approval. The asymmetry between operator fee floors and resident royalty floors identified in prior drafts is hereby resolved: both are inflation-protected on identical terms.

(2) Small covered operator de minimis threshold. A covered operator with estimated Colorado-nexus annual gross revenue below one million dollars ($1,000,000) qualifies for the Small Operator Simplified Compliance pathway:

(a) Simplified registration — annual self-certification in lieu of full covered operator registration, with spot audit authority reserved to the CCPAME;

(b) Reduced metering requirements — quarterly aggregate reporting in lieu of real-time telemetry;

(c) First-year fee waiver — no Enterprise Mitigation fees assessed in the operator's first year of Colorado operation, to avoid creating an entry barrier for emerging Colorado-based AI companies;

(d) Graduated fee ramp — fees assessed at 25% of the statutory rate in year two, 50% in year three, 75% in year four, and 100% in year five and thereafter; and

(e) The de minimis threshold does not apply to operators who have violated any provision of this act or whose Colorado-nexus revenue exceeds $1,000,000 in any subsequent year.

(3) Civic Access Terminal population coverage mandate. The one-terminal-per-county minimum established in §24-20-124 is supplemented by a population coverage mandate:

(a) Each county shall maintain not fewer than one Civic Access Terminal per fifteen thousand (15,000) residents, rounded up — ensuring that high-population counties have proportional access;

(b) Each terminal shall maintain a minimum uptime of ninety-eight percent (98%) in any rolling thirty (30) day period, reported quarterly on the Public Accountability Dashboard;

(c) Counties with fewer than five thousand (5,000) residents qualify for a Rural Hardship Supplement funded from Enterprise Mitigation Revenue — covering the full cost of one Civic Access Terminal and its maintenance, connectivity, and staffing by a part-time Digital Rights Navigator; and

(d) Every Civic Access Terminal shall be physically accessible under the Americans with Disabilities Act, available in all languages required under §24-20-155 accessibility standards, and operable without internet connectivity through a local cache of essential ALAM functions including Police Encounter Protocol and basic rights information.

ADDITIONAL STRENGTHENING PROVISIONS — SINGLE-SUBJECT ANALYSIS

The following provisions substantially increase the bill's gravity while remaining within the single subject of regulating covered automation activity for the protection and benefit of Colorado residents:

Provision	What It Does	Single-Subject Nexus	Gravity Impact
Multi-Domain Pattern of Conduct Aggregation §10-10-302(5)	Assembles violations across all legal domains into unified pattern of conduct claim — solves the multi-case lawyer rejection problem	Enforcement of Digital Soul property rights necessarily requires a mechanism to address multi-domain violations — the same actor who scrapes data also	Transforms the AI attorney from a single-claim tool into a comprehensive legal equalizer. A resident facing housing + civil rights + building code violations files everything simultaneously with one tap. Bad actors face

		retaliates; the enforcement must match the violation	coordinated multi-forum exposure for the first time.
Building Code and Occupancy Whistleblower Integration §10-10-302(6)	Cross-references resident's structure against permit database — identifies unpermitted modifications, occupancy violations, kitchenette upgrades without permits — auto-files whistleblower notice	Covered operators include entities operating AI-assisted building management and occupancy systems — building code compliance is within the scope of automation externalities	Gives every resident in a non-compliant structure instant whistleblower status. Unpermitted kitchenette upgrades, vintage occupancy certificates, and use classification conflicts become immediate leverage. Structural defect discovery triggers simultaneous complaint filing across all venues.
Civic AI Exchange Protocol §10-10-302(8)-(9)	Machine-to-machine communication between resident AI and officer body camera — one-directional — dual cryptographic record — tiered warnings logged in both systems	Police Encounter Protocol is enforcement infrastructure for Digital Soul property rights — law enforcement access to Digital Soul data requires consent framework enforcement at point of contact	Every police encounter becomes a dual-verified record. Officer body cameras log that legal standards were transmitted and received. Discrepancies between Trust and body camera records auto-flag in Pattern Database. Systemic patterns become visible in 90 days.
Absolute Work Product Protection §10-10-303(3)-(4)	Live Legal Mode session records are absolute work product — no exceptions — no warrant reaches them — crime-fraud exception inapplicable by statutory design	AI utility operating as authorized agent in anticipation of legal proceedings generates work product — Hickman v. Taylor applies — the function determines the protection not the tool	The AI attorney's notes are permanently sealed. Prosecutors cannot access what the resident told their AI before arrest. Police encounter recordings in the Trust are off limits to everyone except the resident and their attorney. True attorney-equivalent protection for people who can't afford attorneys.
Encryption Backdoor Prohibition §10-10-303(7)	Categorical prohibition on mandated backdoors, government keys, and exceptional access mechanisms	A Digital Soul property right with a government backdoor is not a property right — the prohibition is constitutionally necessary to give the right meaning	Stronger than Apple v. FBI. No court order, no national security letter, no federal mandate can require a backdoor into the AI utility. Colorado's sovereign power to protect property rights shields residents from federal overreach.
Operator Loyalty Obligation §10-10-303(6)	AI utility owes exclusive loyalty to owner — cannot be commandeered, redirected, or operated against owner — $50K per violation damages	Covered operator relationship with resident is the subject of the act — loyalty obligation is a condition of operating a utility in Colorado	The AI cannot be turned against its owner by anyone for any reason. No secret government mode. No operator selling usage patterns. No employer demanding access. $50K damages per violation makes enforcement economically rational.

AMPLIFY ACT v28 — RESIDENTIAL AI GATEWAY

SECTION 10-10-305. RESIDENTIAL AI GATEWAY DEVICE — CIVIC UTILITY PERIMETER INFRASTRUCTURE — EDGE-COMPUTED COMPLIANCE — FOURTH AMENDMENT ARCHITECTURAL STANDARD — 30-DAY SYMMETRICAL NOTICE

10-10-305. Residential AI Gateway Device — establishment as Civic Utility physical infrastructure — mandatory perimeter enforcement — edge-computed Synthetic Data Integrity Marker processing — violation-alert-only transmission — no raw data egress — 30-day installation notice — 30-day cure period — physical mechanical override — Joint Household Consent interface — import compliance pathway — Pre-Digital Mechanical Asset compatibility — constitutional Fourth Amendment architectural compliance.

(1) Legislative findings. The general assembly finds and declares that:

(a) Regulating the internal hardware of AI devices manufactured outside Colorado or the United States is constitutionally precarious under the Dormant Commerce Clause, practically impossible as an enforcement matter, and creates an unlevel playing field between domestic and imported devices — whereas regulating the perimeter of the Colorado home through a mandated standardized gateway device resolves all three problems simultaneously;

(b) A Residential AI Gateway Device — a standardized, CCPAME-certified network gateway through which all covered AI devices in a Colorado residence must route — constitutes the physical infrastructure of the Civic Utility, analogous to an electric meter box: it does not regulate what devices are built abroad; it regulates how those devices connect to Colorado's digital infrastructure when they enter a Colorado home;

(c) Edge-computed compliance — in which the Residential AI Gateway Device processes Synthetic Data Integrity Markers, Hash-Sentinel verification, and Non-Networked Isolation Protocol enforcement locally, transmitting only cryptographic violation alerts rather than raw data — satisfies the Fourth Amendment concerns raised in smart meter surveillance cases including Naperville Smart Meter Awareness v. City of Naperville by ensuring that the intimate details of residential digital activity never leave the home in identifiable form;

(d) A physical mechanical override — a hardwired switch giving the resident the ability to completely and instantly sever all covered device network connectivity — is the physical expression of the resident's Non-Networked Isolation Protocol right and the home sanctuary principle, ensuring that no software command, remote instruction, or covered operator action can override the resident's physical control of their own home network; and

(e) The 30-day symmetrical notice standard — 30 days from operator notification to resident for installation scheduling, and 30 days from ODO violation notice to operator

for cure — creates a balanced compliance framework that gives residents adequate time to participate in installation without disruption and gives operators adequate time to cure technical violations without punitive immediate enforcement.

(2) Residential AI Gateway Device — definition and required functions. A 'Residential AI Gateway Device' (RAGD) is a CCPAME-certified network gateway device, provided at no cost to the resident, that:

(a) Sits at the network perimeter of the Colorado residence — between the internet service provider's connection point and all covered AI devices operating within the residence — through which all covered device network traffic must route;

(b) Enforces the Non-Networked Isolation Protocol at the network perimeter — implementing hardware-level circuit-break and physical disconnection capability for covered devices based on the resident's Master Deed settings, without requiring software commands from covered operators;

(c) Processes Synthetic Data Integrity Markers and Hash-Sentinel verification locally on the device — edge-computed, never transmitted — comparing covered device output patterns against the resident's registered baseline and flagging anomalies without sending raw residential data to any external system;

(d) Transmits only cryptographic violation alerts — not raw data, not behavioral patterns, not content — to the Colorado Trust of Unique and Identifying Information when a Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is confirmed; the alert contains only: a timestamp, a device identifier hash, a violation category code, and a cryptographic proof of the violation — sufficient for enforcement, insufficient for surveillance;

(e) Routes Base Dividend data generation at Tier 1 — anonymous aggregate telemetry sufficient to establish the resident's entitlement to the Base Dividend — processed and anonymized locally before any transmission, such that no identifying information is transmitted in connection with Base Dividend generation;

(f) Authenticates Premium Royalty entitlement at Tier 2 — identifying the resident's Master Deed and the covered operator's Token Output Attribution Charge obligation — through a cryptographic handshake that confirms identity without transmitting behavioral content;

(g) Maintains a local encrypted log of all covered device network activity accessible only through the resident's Master Deed authentication — the resident has full access to their own home's network log through the Universal Telemetry Allowance; no external party has access to this log except through the warrant and work product procedures of §10-10-303;

(h) Features a physical mechanical override switch — hardwired, not software-controlled — that the resident may engage at any time to completely and instantly sever all covered device connectivity at the network perimeter; the override requires no software command, cannot be disabled remotely, and cannot be overridden by any covered operator instruction or network signal; and

(i) Features a Joint Household Consent Interface — a physical interface on the device allowing all adult residents of the household to register consent preferences independently — implementing the household consent architecture of §15-15-165.

(3) 30-Day symmetrical notice standard — installation. The RAGD deployment process operates on a 30-day symmetrical notice standard:

(a) Operator to resident — 30-day installation notice: A covered operator whose AI devices operate in Colorado residences shall provide the resident with not fewer than thirty (30) days written notice before any scheduled RAGD installation or upgrade. The notice shall include: the installation date and time window; the identity of the certified installer; the resident's right to reschedule within the 30-day window; and the resident's right to request a Civic Access Terminal-assisted installation at no cost if the resident cannot accommodate a home visit;

(b) ODO to operator — 30-day cure period: Upon the ODO's issuance of a RAGD compliance violation notice to a covered operator — for failure to deploy, failure to certify, failure to maintain, or RAGD technical deficiency — the covered operator has thirty (30) days to cure the identified violation before any enforcement penalty is assessed. The cure period is a single 30-day window — not renewable — after which daily penalties accrue under Annex E;

(c) Symmetry rationale: The 30-day window runs identically in both directions — 30 days for the operator to give the resident notice before installation, and 30 days for the operator to cure after receiving an ODO violation notice. The resident is never given less notice than the operator receives.

(4) RAGD as Civic Utility physical infrastructure — regulatory classification. The Residential AI Gateway Device is classified as Civic Utility physical infrastructure for all regulatory purposes:

(a) The RAGD is not the resident's property — it is state-certified Civic Utility infrastructure installed on behalf of the CCPAME, analogous to an electric meter box installed by a utility company on the customer's premises. The resident has the right to use, configure, and physically override the RAGD but does not own it and is not responsible for its maintenance;

(b) The RAGD is the covered operator's compliance infrastructure — the cost of RAGD provision, installation, certification, maintenance, and replacement is a covered operator obligation funded from Enterprise Mitigation Revenue, not a resident cost;

(c) The RAGD's classification as Civic Utility infrastructure means that its installation on residential premises does not constitute a search or seizure within the meaning of the Fourth Amendment — analogous to utility meter installation on private property, which courts have consistently held does not require a warrant. The edge-computed architecture — under which no raw residential data is transmitted — distinguishes the RAGD from smart meter surveillance systems and eliminates the Fourth Amendment concern identified in Naperville; and

(d) The RAGD certification standard is published by the CCPAME and ODO jointly within eighteen (18) months of enactment. Any device meeting the certification standard may serve as a RAGD — the standard is open and technology-neutral, not proprietary to any manufacturer.

(5) Import compliance pathway — foreign-manufactured covered devices. A covered AI device manufactured outside Colorado or the United States:

(a) Is not required to contain any Colorado-specific hardware, firmware, or software compliance capability — the RAGD handles perimeter enforcement regardless of the device's internal architecture;

(b) Must be registered in the CCPAME's Covered Device Registry by the covered operator before being marketed or sold for use in Colorado residences — registration requires only a device identifier, a technical description, and the covered operator's certification that the device will operate through a RAGD in Colorado residential deployments;

(c) Is treated as compliant with all Colorado covered device technical standards once it operates through a certified RAGD — the RAGD is the compliance point, not the device; and

(d) If a covered device is specifically engineered to circumvent, bypass, tunnel around, or otherwise defeat RAGD perimeter enforcement — including through encrypted side-channel transmissions, peer-to-peer connectivity that bypasses the residential network, or hardware-level direct cellular connectivity — the device is a Prohibited Circumvention Device subject to immediate import prohibition, market withdrawal, and Critical Severity Violation enforcement against the covered operator.

(6) Pre-Digital Mechanical Asset compatibility. The RAGD shall not interfere with, monitor, or connect to any certified Pre-Digital Mechanical Asset as defined in §15-15-160. The RAGD's perimeter enforcement applies exclusively to covered AI devices — digital, networked, or AI-enabled equipment. A Pre-Digital Mechanical Asset that has no network connectivity is outside the RAGD's operational scope by definition and no covered operator may use the RAGD to monitor, track, or collect data about Pre-Digital Mechanical Assets operating within the residence.

(7) Enforcement — RAGD non-deployment and circumvention. A covered operator that:

(a) Fails to deploy a certified RAGD in a Colorado residence where covered AI devices are operating, after the 30-day cure period: daily administrative penalty of one thousand dollars ($1,000) per residence per day;

(b) Deploys a non-certified RAGD or a RAGD that fails certification standards: Tier 2 Digital Severance violation;

(c) Markets, sells, or deploys a Prohibited Circumvention Device in Colorado: Critical Severity Violation, immediate market withdrawal, and disgorgement of all revenue from Colorado sales of the device; and

(d) Accesses the resident's local RAGD network log without the resident's consent or a valid warrant: $50,000 per access plus attorney fees under §10-10-303(6).

SECTION 15-15-165. HOME SANCTUARY GATEWAY RIGHTS — PHYSICAL MECHANICAL OVERRIDE — JOINT

HOUSEHOLD CONSENT — MASTER DEED CONTROL — RAGD AS PROPERTY RIGHT INSTRUMENT

15-15-165. Home Sanctuary Gateway Rights — Residential AI Gateway Device as instrument of the resident's Digital Soul property right — physical mechanical override as inalienable right — Joint Household Consent architecture — no covered operator override authority — resident RAGD configuration rights — home as digital sanctuary.

(1) RAGD as instrument of the Digital Soul property right. The Residential AI Gateway Device installed in a Colorado residence is the physical instrument through which the resident exercises their Digital Soul property rights within the home. The resident's RAGD configuration rights are an extension of their Digital Soul property rights under this article and are inalienable.

(2) Physical mechanical override — inalienable right. Every Colorado resident in whose residence a RAGD is installed has the inalienable right to engage the RAGD's physical mechanical override at any time, for any reason, without notice, without explanation, and without consequence:

(a) Engaging the physical mechanical override instantly and completely severs all covered device network connectivity at the residential network perimeter — no covered device in the residence can transmit or receive data through any channel controlled by the RAGD;

(b) No covered operator, state agency, court order, or any other authority may require a resident to disengage the physical mechanical override, penalize a resident for engaging it, condition any service or benefit on the resident's agreement not to engage it, or remotely disable or circumvent it;

(c) The physical mechanical override is hardwired — it operates through physical circuit interruption, not software — ensuring that no firmware update, remote command, network signal, or software exploit can defeat it; and

(d) Engaging the physical mechanical override does not suspend, reduce, or affect the resident's Master Deed registration, Base Dividend entitlement, Premium Royalty accrual, or any other right under this article or title 24, article 20 — the resident's rights continue to accrue during any period of override engagement.

(3) Joint Household Consent architecture. For residences occupied by more than one adult Colorado resident:

(a) The RAGD's Joint Household Consent Interface allows each adult resident to register independent consent preferences for each covered device and each covered operator operating through the RAGD;

(b) The RAGD enforces the most restrictive consent setting among all adult residents for any given covered device or covered operator — if one adult resident has restricted a covered operator's access, that restriction applies to all network traffic through the RAGD regardless of other residents' settings;

(c) No adult resident's consent preferences may be modified by another resident — each adult resident's settings are independently authenticated through their individual Master Deed credential;

(d) A covered operator seeking to change the consent settings applicable to a residence must obtain affirmative consent from every adult resident independently — bundled consent, default-on consent, and implied consent are prohibited at the household level; and

(e) The physical mechanical override may be engaged by any adult resident independently — one resident's decision to engage the override protects the entire household, regardless of other residents' preferences.

(4) RAGD configuration rights — resident control. The resident's RAGD configuration rights include:

(a) The right to set individual consent permissions for each covered device and covered operator at any level of granularity — by data category, by time period, by purpose, or by blanket permission or restriction;

(b) The right to access the RAGD's local encrypted network log through the Universal Telemetry Allowance at any time — seeing a complete record of all covered device network activity within the residence;

(c) The right to configure the RAGD to activate the Non-Networked Isolation Protocol automatically based on time schedules, device behavior triggers, or network anomaly detection;

(d) The right to designate specific rooms, spaces, or times as Non-Networked Zones within the residence — areas where the RAGD enforces complete covered device connectivity severance regardless of device-level settings; and

(e) The right to receive plain-language real-time notifications through the myColorado platform or the RAGD's local interface when any Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is detected within the residence — without any raw data leaving the home.

(5) Home as digital sanctuary — no warrantless RAGD access. The RAGD, its local network log, and all data processed by the RAGD within the residence are entitled to the full home sanctuary protections of the Fourth Amendment to the United States Constitution and Article II, Section 7 of the Colorado Constitution. The home's digital perimeter — as enforced by the RAGD — is the digital equivalent of the physical threshold of the home, crossing which requires a warrant. No government agency, law enforcement body, covered operator, or third party may access the RAGD's local log, query the RAGD's settings, or obtain any information about the RAGD's operation within the residence except pursuant to a warrant meeting the requirements of §10-10-303(5), served on the ODO through the Colorado Trust of Unique and Identifying Information — not on the covered operator and not on the RAGD directly.

RAGD ARCHITECTURAL SUMMARY — CONSTITUTIONAL DEFENSIBILITY ANALYSIS

Element	Design Feature	Constitutional Problem Solved	Strategic Effect
Perimeter regulation not device regulation	RAGD sits between ISP and home network — all foreign devices comply automatically by routing through it	Dormant Commerce Clause — state cannot regulate design of foreign-manufactured goods; can regulate utility access within state	No fight with Apple, Samsung, or Huawei about hardware redesign. They just have to route through the meter box. Every AI device on earth becomes instantly compliant.
Edge-computed compliance	Synthetic Data Integrity Markers and Hash-Sentinels processed locally — only cryptographic violation alerts transmitted, never raw data	Fourth Amendment smart meter concern — Naperville held granular home data transmission is a search. No raw data leaves = no search	Raw residential behavior stays in the home. The CCPAME knows a violation occurred — not what caused it. Law enforcement cannot mine RAGD data for behavioral surveillance.
Violation-alert-only transmission	Alert contains only: timestamp, device hash, violation category code, cryptographic proof — nothing else transmitted	Minimization requirement — any surveillance system must collect no more than necessary. Four data points is the minimum necessary for enforcement	Even with a warrant, the Trust only has four data points per alert. There is nothing else to produce. The architecture makes mass surveillance technically impossible.
Physical mechanical override	Hardwired circuit interruption — no software, no remote defeat, no operator override	Griswold penumbra — the home has a zone of privacy that government cannot penetrate; physical override is the resident's absolute control of that zone	No one can turn the resident's home network back on remotely. Not the operator. Not the government. Not a court order. The switch is physical. Physics is the law.
30-day symmetrical notice	30 days operator-to-resident before installation; 30 days operator-to-cure after ODO notice	Due process — adequate notice before enforcement; symmetry prevents government from giving residents less notice than operators receive	Equal notice both ways. Operators cannot ambush residents with installation. ODO cannot sanction operators without a cure window. Balanced, defensible, fair.
Import compliance pathway	Foreign devices comply through routing, not redesign — Prohibited Circumvention Device classification for deliberate bypass	Supremacy Clause and WTO — state cannot mandate foreign product redesign; can prohibit circumvention of domestic utility infrastructure	Every AI device in the world is either compliant by default (routes through RAGD) or a prohibited circumvention device. There is no middle ground and no foreign-manufacturer carve-out.

AMPLIFY Act v28 — §10-10-305 Residential AI Gateway Device · §15-15-165 Home Sanctuary Gateway Rights Civic Utility Perimeter Infrastructure · Edge-Computed Compliance · Physical Mechanical Override · Joint Household Consent · 30-Day Symmetrical Notice · Import Compliance Pathway

AMPLIFY ACT v28 — BILLS 2 & 3 RESILIENCE & EXPANSION SECTIONS

§§10-10-305 through 10-10-306 · §§24-20-163 through 24-20-170

Quantum Cryptography · Open API · Anti-Concentration · Revenue Floor · Municipal Bonds · Infrastructure Investment · Cross-State Reciprocity · Workforce Transition · Premium Royalty Market

SECTION 10-10-305. CRYPTOGRAPHIC STANDARDS EMERGENCY UPGRADE AUTHORITY — POST-QUANTUM READINESS — TRUST INFRASTRUCTURE RESILIENCE

10-10-305. Cryptographic Standards Emergency Upgrade Authority — ODO authority to upgrade Trust cryptographic standards without legislative action — NIST post-quantum certification trigger — 90-day implementation mandate — covered operator upgrade obligation — legacy system sunset.

(1) Legislative finding. The general assembly finds that: (a) Current cryptographic standards — including those certified under FIPS 140-2 Level 3 — are vulnerable to quantum computing attacks that are projected to become operationally feasible within the operational lifespan of the Colorado Trust of Unique and Identifying Information; (b) NIST has published post-quantum cryptographic standards (FIPS 203, 204, 205) and will publish additional standards as the field develops; (c) Requiring legislative action to upgrade Trust cryptographic standards would create a window of vulnerability between NIST certification and legislative implementation that adversarial actors could exploit; and (d) The ODO must have standing authority to upgrade Trust cryptographic standards in response to NIST publications without awaiting legislative action — the same way the state upgrades software patches without legislative approval.

(2) Cryptographic Standards Emergency Upgrade Authority. The ODO has standing authority — without legislative action, CCPAME board vote, or executive order — to upgrade the cryptographic standards of the Colorado Trust of Unique and Identifying Information within ninety (90) days of NIST publishing any post-quantum cryptographic standard designated as applicable to sensitive government data systems. The upgrade authority: (a) Covers all cryptographic functions within the Trust — data encryption at rest, data encryption in transit, identity verification hash generation, session authentication, and digital signature standards; (b) Requires the ODO to publish a Cryptographic Upgrade Notice on the Public Accountability Dashboard simultaneously with the upgrade deployment; (c) Triggers a corresponding covered operator upgrade obligation — every certified covered operator must implement the upgraded cryptographic standards within one hundred eighty (180) days of the ODO's Cryptographic Upgrade Notice; and (d) Does not require the ODO to maintain backward compatibility with pre-upgrade standards beyond a twelve (12) month transition period.

(3) Quantum-resistant architecture mandate. Within thirty-six (36) months of enactment, the ODO shall: (a) Complete a full post-quantum readiness assessment of all Trust cryptographic infrastructure; (b) Publish a Post-Quantum Migration Plan on the Public Accountability Dashboard; (c) Implement hybrid classical-quantum resistant encryption for all Trust data at rest; and (d) Require all certified covered operators to certify post-quantum readiness as a condition of annual registration renewal beginning in the fourth year after enactment.

(4) Legacy system sunset. Any covered operator cryptographic system that has not been upgraded to current Trust cryptographic standards within twenty-four (24) months of a Cryptographic Upgrade Notice is automatically suspended from receiving new resident Decentralized Identity Verification Protocol consents until compliance is certified. Existing resident data held in non-compliant systems triggers an Operator Exit Event under §15-15-166 for the non-compliant data category.

SECTION 10-10-306. CCPAME OPEN API MANDATE — THIRD-PARTY DEVELOPER ECOSYSTEM — PUBLIC DATA ACCESSIBILITY — INNOVATION PLATFORM DESIGNATION

10-10-306. CCPAME Open API mandate — public data accessibility — third-party developer ecosystem — API certification — privacy-preserving data access — innovation platform designation — prohibited commercial exploitation.

(1) Open API mandate. Within twenty-four (24) months of enactment, the CCPAME and ODO shall publish and maintain open application programming interfaces (APIs) for the following public data systems: (a) The Public Accountability Dashboard — all publicly reported aggregate data in machine-readable format, updated in real time consistent with Dashboard update schedules; (b) The Legal Violation Pattern Database — anonymized aggregate violation data by category, geography, and actor type, updated quarterly; (c) The Environmental Impact Panel — aggregate energy consumption, renewable percentage, water consumption, and ORC output data, updated in real time; (d) The Civic Access Terminal network status — uptime, location, and accessibility status of all terminals, updated hourly; (e) The covered operator registry — name, registration status, industry classification, and compliance history of all registered covered operators; and (f) The Resident Data Cooperative registry — name, membership size, certification status, and collective negotiation outcomes of all certified cooperatives.

(2) API standards and certification. All CCPAME Open APIs shall: (a) Comply with REST or GraphQL architectural standards; (b) Provide data in JSON and CSV formats without proprietary encoding; (c) Require API key registration — free, available to any person or entity, with rate limits sufficient to support commercial application development; (d) Include complete technical documentation published on the CCPAME developer portal; and (e) Maintain ninety-nine percent (99%) uptime with a public status page showing real-time API availability.

(3) Third-party developer ecosystem. The CCPAME shall designate its public data infrastructure as an Innovation Platform and: (a) Publish annual developer challenges with prize funding from Enterprise Mitigation Revenue — not to exceed one-tenth of one percent (0.1%) of annual revenue — for applications that increase resident benefit from the AMPLIFY Act ecosystem; (b) Maintain a public application registry where certified third-party developers list consumer applications built on CCPAME APIs; and (c) Certify third-party applications that meet privacy, security, and accuracy standards — certified applications may display a CCPAME Certified seal.

(4) Prohibited commercial exploitation. Third-party API access does not grant any right to: (a) Re-identify anonymized data; (b) Build commercial data products that compete with CCPAME core functions; (c) Use CCPAME data to target covered operators with competitive intelligence products; or (d) Access any resident-specific data — all API data is aggregate and anonymized. Violations result in permanent API access revocation and referral to the Colorado Attorney General.

SECTION 24-20-163. ANTI-CONCENTRATION RATE TRIGGER — DOMINANT MARKET OPERATOR DESIGNATION — MARKET STRUCTURE REVIEW — ATTORNEY GENERAL REFERRAL

24-20-163. Anti-concentration rate trigger — Dominant Market Operator designation — 35% Colorado-nexus token output threshold — 1.25x fee multiplier — 50% threshold market structure review — Attorney General antitrust referral — board conflict-of-interest enhanced restrictions.

(1) Legislative finding. The general assembly finds that extreme market concentration among covered operators creates regulatory capture risk — a single covered operator controlling the majority of Colorado-nexus AI output has disproportionate leverage to challenge fee structures, complicate compliance standards, and capture the CCPAME board through coordinated political pressure. An automatic rate multiplier triggered by concentration above defined thresholds creates a structural disincentive to monopolistic consolidation without requiring case-by-case regulatory action.

(2) Dominant Market Operator designation. A covered operator whose Colorado-nexus annual token output exceeds thirty-five percent (35%) of the total Colorado-nexus annual token output across all registered covered operators is automatically designated a Dominant Market Operator. Dominant Market Operator designation: (a) Triggers a 1.25x multiplier on all §24-20-156 base fee rates — applied to the Dominant Market Operator's full Colorado-nexus output, not just the portion exceeding the 35% threshold; (b) Triggers enhanced board conflict-of-interest restrictions — no person with any current or prior employment, ownership, consulting, or contractual relationship with the Dominant Market Operator or any of its affiliates within the prior five (5) years may serve on the CCPAME Board of Directors, the ODO Advisory Panel, or any CCPAME rate-setting committee; (c) Triggers a mandatory annual market structure report published on the Public Accountability Dashboard showing the operator's Colorado-nexus market share, fee contribution, and any changes in concentration; and (d) Is automatically removed when the operator's Colorado-nexus market share falls below 30% for two consecutive calendar years.

(3) 50% threshold — market structure review and AG referral. If any covered operator's Colorado-nexus annual token output exceeds fifty percent (50%) of total Colorado-nexus output: (a) The CCPAME shall initiate a mandatory Market Structure Review within sixty (60) days; (b) The CCPAME shall refer the market concentration data to the Colorado Attorney General for antitrust analysis under C.R.S. §6-4-101 et seq.; (c) The Attorney General shall respond within ninety (90) days with a determination whether to open an antitrust investigation; and (d) The 1.25x Dominant Market Operator multiplier increases to 1.5x for the period of the Market Structure Review and any subsequent antitrust investigation.

SECTION 24-20-164. ENTERPRISE MITIGATION REVENUE FLOOR GUARANTEE — AUTOMATIC RATE REVIEW TRIGGER — DYNAMIC ADJUSTMENT ACCELERATION — OPERATOR EXIT DETERRENCE

24-20-164. Enterprise Mitigation Revenue floor guarantee — 75% prior-year collection floor — automatic Dynamic Rate Adjustment Protocol acceleration trigger — CCPAME emergency rate review — revenue collapse deterrence — operator exit penalty.

(1) Revenue floor guarantee. If annual Enterprise Mitigation Revenue in any fiscal year falls below seventy-five percent (75%) of the prior fiscal year's total Enterprise Mitigation Revenue collections — whether due to operator exit, fee avoidance, revenue base erosion, or any other cause — the following automatic responses are triggered without CCPAME board action:

(a) The Dynamic Rate Adjustment Protocol under §24-20-156(4) activates immediately — not at the next annual cycle — and the CCPAME initiates an emergency rate review within thirty (30) days;

(b) The Mandatory Investment Reserve floor under §24-20-154(2)(a) is suspended for the affected fiscal year — the full Overflow Pool is available for Resident Mitigation Dividend distribution to maintain resident payment continuity;

(c) The CCPAME publishes a Revenue Shortfall Notice on the Public Accountability Dashboard within fifteen (15) days of detecting the shortfall, identifying the revenue gap and projected impact on resident distributions; and

(d) The Colorado Attorney General is automatically notified and shall investigate whether the revenue decline resulted from coordinated operator conduct constituting tortious interference with the CCPAME's revenue base or antitrust violations.

(2) Operator exit deterrence — exit penalty. A covered operator that voluntarily exits the Colorado market — ceasing all Colorado-nexus covered automation activity — within five (5) years of its first covered operator registration is subject to an Operator Exit Penalty: (a) Equal to fifty percent (50%) of the operator's average annual Enterprise Mitigation fee contribution over the period of its registration, multiplied by the number of years remaining in the five-year period; (b) Payable to the CAMT Investment Reserve within ninety (90) days of the exit event; (c) Collectible as a civil judgment in Colorado courts; and (d) Not applicable to operators exiting due to insolvency under §15-15-166 — the exit penalty applies only to voluntary, solvent exits designed to avoid fee obligations.

SECTION 24-20-165. CCPAME REVENUE BOND AUTHORITY — MUNICIPAL BOND MARKET ACCESS — INFRASTRUCTURE CAPITAL — MARKET CONSTITUENCY CREATION

24-20-165. CCPAME revenue bond authority — Enterprise Mitigation Revenue-backed bonds — investment-grade rating mandate — permitted uses — bondholder protections — market constituency creation — General Fund non-recourse.

(1) Legislative finding. The general assembly finds that: (a) CCPAME revenue bond authority transforms the enterprise from a regulatory agency into a capital markets participant — investment banks, pension funds, and municipal bond investors become financially invested in CCPAME's revenue base, creating a powerful private-sector constituency defending Enterprise Mitigation Revenue against political erosion; (b) Revenue bonds backed by Enterprise Mitigation Revenue provide capital for infrastructure investment — Civic Access Terminal expansion, Trust infrastructure upgrades, ORC system financing, workforce transition programs — before revenue accumulates to fund those investments from cash flow; (c) CCPAME revenue bonds are not general obligation bonds — the State of Colorado's credit is not pledged and the General Fund bears no repayment obligation.

(2) Revenue bond authority. The CCPAME is authorized to issue revenue bonds, notes, and other obligations secured by a pledge of Enterprise Mitigation Revenue, subject to: (a) A maximum outstanding principal balance not exceeding thirty percent (30%) of the prior fiscal year's total Enterprise Mitigation Revenue; (b) A debt service coverage ratio covenant of not less than 1.5x — annual Enterprise Mitigation Revenue must exceed annual debt service by at least 50%; (c) Investment-grade rating from at least two nationally recognized statistical rating organizations before any bond issuance — the rating process is itself a public validation of the CCPAME's financial health; (d) A public bond issuance plan approved by the CCPAME Board of Directors and published on the Public Accountability Dashboard thirty (30) days before issuance; and (e) Proceeds restricted to permitted uses under subsection (3) — bond proceeds may not supplement operating revenues or fund resident distributions.

(3) Permitted bond uses. CCPAME revenue bond proceeds may be used exclusively for: (a) Civic Access Terminal network expansion and upgrade; (b) Colorado Trust of Unique and Identifying Information infrastructure construction, upgrade, and post-quantum cryptographic migration; (c) ORC thermal recapture system construction financing under §24-20-143; (d) Civic Enforcement Access Terminal network build-out; (e) Workforce Transition Account infrastructure under §24-20-169; and (f) Refinancing of outstanding CCPAME obligations at lower interest rates.

(4) General Fund non-recourse. CCPAME revenue bonds are payable solely from Enterprise Mitigation Revenue pledged to bond repayment. The State of Colorado, the General Fund, and the Colorado Automation Mitigation Trust bear no liability for CCPAME revenue bond repayment. Bond documents shall prominently disclose this non-recourse character. No state official may pledge state credit to support CCPAME revenue bond repayment without a constitutional amendment.

SECTION 24-20-166. COLORADO INFRASTRUCTURE INVESTMENT AUTHORITY — INVESTMENT RESERVE DIRECT INVESTMENT — SOVEREIGN WEALTH FUND MODEL — DOUBLE RETURN ARCHITECTURE

24-20-166. Colorado Infrastructure Investment Authority — Investment Reserve direct investment in Colorado infrastructure — permitted infrastructure categories — return-generating requirements — UFIPA income stream integration — double return architecture — rural broadband priority.

(1) Legislative finding. The general assembly finds that: (a) The Investment Reserve currently holds exclusively financial instruments — bonds, treasuries, and income-producing securities; (b) Direct investment in Colorado infrastructure — rural broadband, water treatment, renewable energy, affordable housing — generates both financial returns flowing through the UFIPA pipeline to residents and direct service improvements serving those same residents; (c) Technology companies whose data extraction funds the Investment Reserve are the same companies whose infrastructure demands — power, water, connectivity — strain Colorado's public infrastructure; routing Investment Reserve returns into that infrastructure closes the loop between extraction and restoration; and (d) The Alaska Permanent Fund, Norway Government Pension Fund Global, and similar sovereign wealth funds have demonstrated that permanent endowment funds can generate superior long-term returns through diversified direct investment while maintaining liquidity for distributions.

(2) Direct infrastructure investment authority. The CCPAME Investment Committee — a subcommittee of the Board of Directors established under subsection (3) — may allocate up to twenty-five percent (25%) of the Investment Reserve to direct investment in Colorado infrastructure projects meeting the criteria of subsection (4). Infrastructure investments are treated as Investment Reserve principal for UFIPA purposes — their returns are Net Income Receipts flowing through §24-20-157 to residents as UFIPA Income Distributions.

(3) Investment Committee. The CCPAME Board shall establish an Investment Committee of not fewer than five (5) members including: (a) Not fewer than two (2) members with demonstrated professional investment management experience; (b) Not fewer than one (1) member with infrastructure finance experience; (c) Not fewer than one (1) member representing rural Colorado communities; and (d) Not fewer than one (1) registered Master Deed holder elected by the Master Deed holder population through a process administered by the Secretary of State. No CCPAME Board member with a conflict of interest in any investment under consideration may participate in the Investment Committee vote on that investment.

(4) Permitted infrastructure investment categories. The Investment Reserve may be directly invested in: (a) Rural broadband infrastructure — priority given to Colorado counties with less than 25 Mbps median download speed serving residential addresses; (b) Water treatment and conservation infrastructure — including advanced metering, recycled water systems, and agricultural water efficiency projects — priority given to projects in watersheds affected by covered compute facility water consumption under §24-20-150; (c) Renewable energy generation and storage — solar, wind, geothermal, and pumped hydro projects with a minimum 20-year power purchase agreement with a Colorado utility or municipal power authority; (d) Affordable housing construction and preservation — projects meeting HUD affordability standards in Colorado communities where covered compute facility presence has increased housing cost burdens; and (e) Public transit infrastructure in communities with major covered compute facility concentrations — reducing the transportation externality of large-scale employment centers that do not provide adequate transit access.

(5) Return requirement. Every direct infrastructure investment must: (a) Generate a projected annual return of not less than the Investment Reserve's current blended yield on financial instruments — direct investment must not dilute the Investment Reserve's income-generating performance; (b) Be structured as a loan, equity investment, or revenue

participation — not a grant; and (c) Include a liquidation pathway — the Investment Committee must be able to exit each direct investment within a five-year horizon if required to meet distribution obligations.

SECTION 24-20-167. CROSS-STATE DIGITAL PROPERTY RIGHTS RECIPROCITY — COLORADO STANDARD AS NATIONAL BASELINE — RECIPROCITY CERTIFICATION — MULTI-STATE MASTER DEED RECOGNITION

24-20-167. Cross-state digital property rights reciprocity — CCPAME equivalency certification — Colorado standard as national baseline — mutual Master Deed recognition — reciprocating state resident protections in Colorado — Colorado resident protections in reciprocating states — interstate commerce nexus.

(1) Legislative finding. The general assembly finds that: (a) Colorado is the most advanced digital property rights jurisdiction in the United States and has an opportunity to export its regulatory architecture to other states — establishing Colorado's framework as the de facto national standard before federal legislation preempts state innovation; (b) A reciprocity framework that requires other states to meet Colorado's standard for equivalency certification gives Colorado permanent leverage in the development of national digital property rights norms — states that want Colorado reciprocity must match Colorado's protections; (c) Multi-state Master Deed recognition eliminates the barrier to registration for Colorado residents who also reside or work in other states, and attracts out-of-state residents to register Colorado Master Deeds as the gold standard of digital property rights protection.

(2) CCPAME equivalency certification. The CCPAME shall establish an Interstate Digital Property Rights Equivalency Certification process evaluating other states' digital property rights frameworks against the following minimum standards: (a) An inalienable digital property right in resident data with a definition at least as comprehensive as Colorado's Digital Soul definition; (b) A consent-based data collection framework functionally equivalent to the Decentralized Identity Verification Protocol; (c) An enterprise mitigation fee or equivalent revenue mechanism funding resident distributions; (d) A trust structure protecting distributions from government sweep equivalent to the CAMT's sweep prohibition; (e) An enforcement matrix with statutory damages equivalent to Colorado's Annex E; and (f) An independent administrative enterprise not subject to executive or legislative capture functionally equivalent to the CCPAME.

(3) Reciprocity effects upon certification. Upon CCPAME equivalency certification of a reciprocating state: (a) Colorado Master Deed registrations are recognized in the reciprocating state as equivalent to that state's resident registration — Colorado residents retain their full Colorado Digital Soul rights when their data is processed by covered operators in the reciprocating state; (b) Reciprocating state residents who register Colorado Master Deeds receive Colorado Digital Soul protections for data processed by Colorado-registered covered operators; (c) Covered operators registered in both Colorado and the reciprocating state may satisfy both states' compliance obligations through a unified filing

submitted to both states' administrative enterprises; and (d) The CCPAME publishes a reciprocity status dashboard showing all certified reciprocating states and their equivalency scores relative to Colorado's standard.

(4) Colorado as national standard. The CCPAME shall: (a) Publish an annual National Digital Property Rights Index comparing all U.S. states' digital property rights frameworks against Colorado's standard; (b) Provide technical assistance to other states developing digital property rights legislation — at the requesting state's expense — using Colorado's framework as the template; (c) Participate in the National Conference of State Legislatures digital property rights working group as Colorado's designated representative; and (d) Notify the Colorado congressional delegation when any federal digital property rights legislation is proposed that would preempt Colorado's more protective framework — triggering the CCPAME's standing to appear in any federal legislative or regulatory proceeding affecting Colorado's Digital Soul framework.

SECTION 24-20-168. WORKFORCE TRANSITION ACCOUNT — AUTOMATION DISPLACEMENT RETRAINING — MASTER DEED HOLDER SKILLS ACCOUNT — 5% ENTERPRISE MITIGATION REVENUE ALLOCATION

24-20-168. Workforce Transition Account — automation displacement retraining — Master Deed holder skills account — 5% Enterprise Mitigation Revenue allocation — permitted uses — credential matching — employer co-investment — anti-duplication with existing state programs.

(1) Legislative finding. The general assembly finds that: (a) The covered automation activity taxed under this act is causing real and measurable workforce displacement in Colorado — the same revenue being collected from automation is the appropriate source of funding for the workforce transition that automation is causing; (b) A Workforce Transition Account available to registered Master Deed holders converts displaced workers from opponents of automation — who currently see no benefit flowing to them — into stakeholders in the AMPLIFY Act ecosystem with a direct financial interest in the system's success; (c) A skills account funded from Enterprise Mitigation Revenue is qualitatively different from a cash distribution — it is an investment in the resident's future earning capacity, not a consumption transfer; and (d) Employer co-investment requirements ensure that covered operators who benefit from a skilled Colorado workforce contribute to workforce transition alongside the CCPAME.

(2) Workforce Transition Account — establishment. A Workforce Transition Account is established as a dedicated subaccount of the CAMT, funded at five percent (5%) of annual Enterprise Mitigation Revenue before the Overflow Pool is calculated — treated as a program account ahead of the resident distribution waterfall. The Workforce Transition Account: (a) Is administered by the CCPAME in coordination with the Colorado Department of Labor and Employment; (b) Is available to any registered Master Deed holder who: (I) has experienced documented automation-related job displacement in the prior twenty-four (24) months; (II) is currently employed in an occupation with a documented automation risk score

above 0.7 on the Frey-Osborne or equivalent automation risk index; or (III) is a resident of a Colorado community where covered compute facility deployment has materially altered the local labor market; and (c) Provides each eligible resident with an annual Workforce Transition Credit of not less than five thousand dollars ($5,000) — scaled to documented displacement severity — deposited into the resident's Resident Automated Mitigation Account as a restricted skills account sub-balance.

(3) Permitted uses. Workforce Transition Credits may be used exclusively for: (a) Tuition and fees at any Colorado accredited institution of higher education, community college, or registered apprenticeship program; (b) Industry certification and credentialing programs in fields with documented Colorado labor demand; (c) Equipment and software required for credentialing programs; (d) Childcare costs directly enabling enrollment in qualifying programs — not to exceed thirty percent (30%) of the Workforce Transition Credit; and (e) Transportation costs directly enabling program attendance in rural communities — not to exceed fifteen percent (15%) of the Credit.

(4) Employer co-investment requirement. Any covered operator whose Colorado-nexus annual Enterprise Mitigation fee exceeds five million dollars ($5,000,000) must: (a) Publish an annual Colorado Workforce Transition Plan identifying the operator's projected automation-related workforce impacts in Colorado over the following three years; (b) Contribute to the Workforce Transition Account an amount equal to ten percent (10%) of its annual Enterprise Mitigation fee — in addition to the fee itself — as an employer co-investment; and (c) Preferentially consider Colorado residents with Workforce Transition Credits for open positions in the operator's Colorado operations that match the credentials being pursued. Employer co-investment contributions are credited against the operator's Enterprise Mitigation fee in subsequent years at a rate of fifty cents ($0.50) credit per dollar contributed — creating a direct financial incentive for operator participation.

SECTION 24-20-169. PREMIUM ROYALTY SECONDARY ASSIGNMENT MARKET — CCPAME-REGULATED EXCHANGE — VOLUNTARY RESIDENT ASSIGNMENT — FLOOR PROTECTION — REVOCABILITY — PROHIBITED ASSIGNMENTS

24-20-169. Premium Royalty secondary assignment market — CCPAME-regulated voluntary exchange — maximum 49% assignment — statutory floor protection — 30-day revocability — prohibited assignment categories — anti-predatory assignment rules — resident economic agency.

(1) Legislative finding. The general assembly finds that: (a) Premium Royalty rights are the resident's earned property return from their Digital Soul — they are property rights that, like other property rights, should be usable as economic currency by the resident when the resident chooses; (b) A regulated secondary assignment market — with strong floor protections, mandatory revocability, and categorical prohibitions on predatory assignments — allows residents to use their Premium Royalty rights to access services they value while

maintaining the systemic integrity of the resident distribution architecture; and (c) The assignment market is entirely voluntary — no resident may be required, pressured, or incentivized through service degradation to assign any portion of their Premium Royalty rights.

(2) Secondary assignment market. The CCPAME shall establish and regulate a Premium Royalty Secondary Assignment Market — a regulated exchange through which registered Master Deed holders may voluntarily assign a portion of their future Premium Royalty distributions to certified covered operators, certified cooperatives, or CCPAME-approved service providers in exchange for services, credits, or other consideration. The market operates under the following rules:

(a) Maximum assignment — no resident may assign more than forty-nine percent (49%) of their total Premium Royalty rights across all assignments combined — the resident retains at least 51% of their Premium Royalty regardless of the number or nature of assignments;

(b) Statutory floor protection — no assignment may reduce any single distribution below the statutory Base Dividend floor established in §15-15-110, as CPI-adjusted under §10-10-304(1);

(c) Mandatory 30-day revocability — every assignment is revocable by the resident at any time with thirty (30) days written notice — no assignment may include a lock-up period exceeding ninety (90) days, after which the revocability right is restored;

(d) Assignee certification — only CCPAME-certified assignees may receive Premium Royalty assignments — certification requires demonstration that the consideration offered is fair market value for the Premium Royalty assigned and that no predatory practices are employed; and

(e) CCPAME market oversight — the CCPAME monitors all assignment transactions in real time through the Secondary Assignment Market platform and may suspend any assignee whose practices indicate predatory assignment solicitation.

(3) Prohibited assignments. The following assignments are void and unenforceable regardless of resident consent: (a) Assignments made as a condition of employment, housing, credit, government benefit, or any other necessity of life; (b) Assignments made pursuant to any contract of adhesion or standard-form agreement presented without individualized negotiation opportunity; (c) Assignments to any entity under active CCPAME enforcement action; (d) Assignments of more than six (6) months of future Premium Royalty distributions — the assignment term may not exceed six months, after which a new voluntary assignment must be executed; and (e) Assignments made under circumstances of documented financial distress — the CCPAME shall monitor for distress-driven assignment patterns and may impose a cooling-off period of thirty (30) days before a distress-flagged assignment takes effect.

v28 COMPLETE STRENGTHENING PROVISIONS — SINGLE-SUBJECT ANALYSIS AND GRAVITY IMPACT

Section	Provision	What It Does	Gravity Impact

§15-15-165	Definitional Expansion Clause	CCPAME classifies new data types without legislation — neural interface, ambient, synthetic biology, spatial computing pre-classified at Tier 1/2	Bill never becomes obsolete. Neural interface data captured before Neuralink ships. Technology evolves — bill evolves with it automatically.
§15-15-166	Operator Exit & Wind-Down	Digital Soul data not bankruptcy estate asset — resident election on exit — bankruptcy trustee may not sell resident data — foreign acquisition restriction — CFIUS referral	Closes the most dangerous gap. A Cloudflare-scale bankruptcy can no longer put 3M Colorado residents' Digital Soul on the auction block.
§15-15-167	Bankruptcy Proofing / Asset Immunity	RAMA fully exempt from bankruptcy estate — unlimited exemption — not waivable — judgment creditor restriction — self-settled trust inapplicability	Residents who need protection most — those in financial distress — keep their Digital Soul account intact. The property right is actually inalienable.
§15-15-168	Supermajority Amendment Requirement	2/3 both chambers to amend core provisions — Digital Soul right, distribution architecture, sweep prohibition, enforcement matrix — self-repeals on constitutional ratification	Makes the bill raid-resistant between Phase 1 and Phase 2. A hostile simple majority can't gut the system while the constitutional amendment is circulating.
§10-10-305	Quantum Cryptography Upgrade	ODO upgrades Trust crypto within 90 days of NIST post-quantum certification — no legislative action required — covered operator upgrade obligation — legacy system sunset	Trust stays secure regardless of what computing does. Post-quantum migration is automatic, not legislative.
§10-10-306	CCPAME Open API Mandate	Machine-readable public APIs for Dashboard, Pattern Database, Environmental Panel, operator registry — third-party developer ecosystem — innovation platform	Turns the bill into a platform. Tenant rights apps, wage theft detectors, police encounter analytics — built by developers, maintained by the ecosystem.
§24-20-163	Anti-Concentration Rate Trigger	35% market share = Dominant Market Operator, 1.25x fee multiplier — 50% threshold triggers AG antitrust referral — enhanced board conflict-of-interest rules	Consolidation becomes self-defeating. The bigger one operator gets, the more expensive Colorado becomes for them.
§24-20-164	Revenue Floor Guarantee	75% prior-year collections floor — automatic Dynamic Rate Adjustment acceleration — Investment Reserve floor suspended to protect resident payments — AG notified	Revenue can't collapse faster than the rate structure can respond. Resident checks are protected even during revenue disruption.
§24-20-165	Municipal Bond Authority	CCPAME revenue bonds backed by Enterprise Mitigation Revenue — 30% of prior year revenue cap — 1.5x debt service coverage — investment-grade rating mandate — General Fund non-recourse	Wall Street becomes a defender of Enterprise Mitigation Revenue. Bond ratings are independent public validation of the system's financial health.
§24-20-166	Infrastructure Investment Authority	Investment Reserve direct investment in rural broadband, water, renewable energy, affordable housing — sovereign wealth fund model — return requirement — double return architecture	Same revenue that mitigates automation externalities funds the infrastructure those externalities degrade. Double return: financial yield + direct service improvement.
§24-20-167	Cross-State Reciprocity	CCPAME certifies equivalent state frameworks — Colorado standard as minimum equivalency bar — multi-state Master Deed recognition — National Digital Property Rights Index	Colorado exports its architecture. Other states match Colorado's standard to get reciprocity. Colorado defines the national baseline.
§24-20-168	Workforce Transition Account	5% of Enterprise Mitigation Revenue — $5K minimum annual credit per eligible displaced worker — employer co-investment 10% of fee	Displaced workers become stakeholders. The companies automating them away fund their

		with 50-cent credit return — skills account not cash	retraining. The system turns opponents into constituents.
§24-20-169	Premium Royalty Secondary Market	Voluntary assignment up to 49% — 30-day revocability always — 6-month term max — prohibited in employment/housing contexts — CCPAME-regulated exchange	Digital Soul property rights become economic currency residents can use while keeping control. The property right gains utility without losing protection.

AMPLIFY ACT v28 — FINAL PRIORITY SECTIONS

§§15-15-170 · 15-15-171 · 15-15-172 · 24-20-171

Voter Data Sovereignty · DNA & Genetic Data Absolute Protection · Quantum Infrastructure Emergency Funding

The state owns the tally. The voter owns the vote. — Voter data, DNA, and quantum security are the three highest-priority protections in this act.

SECTION 15-15-170. VOTER DATA SOVEREIGNTY — THE STATE OWNS THE TALLY — THE VOTER OWNS THE VOTE — VOTER DIGITAL SOUL ABSOLUTE PROTECTION — POLITICAL DATA OPERATOR PROHIBITION

15-15-170. Voter Data Sovereignty — separation of tally from voter — voter's ballot, registration data, voting history, precinct behavioral data, and political profile data are inalienable Digital Soul — state's lawful interest limited to aggregate tally — covered political data operators prohibited — AI-assisted voter targeting — absolute consent requirement — Fourteenth Amendment equal protection foundation.

(1) Legislative findings. The general assembly finds and declares that:

(a) The right to vote is the foundational right of democratic self-governance — and the data generated by the exercise of that right belongs to the voter, not to the state, not to any political party, not to any campaign, not to any data broker, and not to any covered operator processing that data for commercial or political advantage;

(b) There is a precise and legally significant distinction between: (I) the TALLY — the aggregate count of votes cast for each candidate or measure, which is a public governmental record belonging to the People of Colorado collectively; and (II) the VOTE — the individual voter's registration data, party affiliation, voting history, precinct assignment, absentee ballot status, signature data, demographic profile, behavioral data generated through the voting process, and any political preference or behavior data derived from that voter's participation — which is the voter's inalienable Digital Soul at the highest tier of protection;

(c) The commercial political data industry — including voter file vendors, political analytics platforms, campaign technology providers, microtargeting services, and AI-assisted voter persuasion systems — processes Colorado voter data at industrial scale for commercial and political advantage, generating revenue from the voter's most

intimate democratic expression without the voter's meaningful consent and without returning any value to the voter;

(d) AI-assisted voter targeting — the use of machine learning models trained on voter behavioral data to predict, influence, and manipulate individual voting decisions — represents a qualitatively different threat to democratic self-governance than traditional mass advertising, because it operates at the individual level, in real time, with a precision that the individual voter cannot detect or counter;

(e) The voter's Digital Soul data generated through electoral participation is not merely personal property — it is the data substrate of democratic self-governance itself; its commercialization without consent is an injury not just to the individual voter but to the democratic process; and

(f) Voter Data Sovereignty — the principle that the state's lawful interest in electoral data is limited to the aggregate tally, and that all individual voter data belongs to the voter as inalienable Digital Soul — is the digital-era expression of the secret ballot principle established in Colorado law since 1891.

(2) Definitional framework — Voter Digital Soul. For purposes of this section:

(a) 'Voter Digital Soul' means all data uniquely identifying, profiling, or derived from an individual Colorado registered voter's participation in the electoral process, including: (I) voter registration data — name, address, party affiliation, registration date, registration status; (II) voting history — whether the voter voted in each election, by what method (in-person, mail, early), at what location; (III) ballot request and return data — absentee ballot request dates, return dates, cure status; (IV) signature data collected through the ballot process; (V) precinct assignment and geographic electoral unit data; (VI) demographic data collected or inferred through the voter registration process; (VII) any behavioral data generated through government-operated voter registration portals, election websites, or voting systems; and (VIII) any political preference, party support, candidate preference, issue position, or electoral behavior data derived or inferred from any of the above through any analytical process;

(b) 'Political Data Operator' means any covered operator that processes Voter Digital Soul data for commercial, political, or analytical purposes — including voter file vendors, political analytics platforms, campaign technology providers, voter contact systems, microtargeting services, AI-assisted voter persuasion systems, and any operator whose covered automation activity includes training models on or generating inferences from Voter Digital Soul data; and

(c) 'State Electoral Tally' means the aggregate count of votes cast for each candidate or ballot measure in each Colorado election — a public governmental record that belongs to the People of Colorado collectively, is subject to public inspection under C.R.S. §24-72-204, and is expressly excluded from Voter Digital Soul.

(3) Voter Digital Soul — inalienable property right at highest protection tier. Voter Digital Soul is the voter's inalienable intangible personal property at Protection Tier 1 — the highest tier under this act — with the following specific attributes:

(a) The voter's Voter Digital Soul may not be processed, sold, transferred, licensed, or used by any political data operator without the voter's affirmative, informed, specific, written consent — a blanket consent to voter file access is not sufficient; consent must specify the exact data categories, the specific operator, the specific electoral purpose, and the specific time period, and must be renewed before each election cycle;

(b) The voter's Voter Digital Soul may not be used for AI-assisted voter targeting, microtargeting, persuasion modeling, sentiment analysis, or any other automated individual-level political influence activity regardless of consent — this prohibition is absolute and is not subject to waiver;

(c) The voter's party affiliation data, candidate preference data, and issue position data derived from Voter Digital Soul processing may not be sold, licensed, or transferred to any third party regardless of consent — these categories are non-transferable;

(d) The voter has a Universal Telemetry Allowance over all Voter Digital Soul data — including all data held by political data operators and the Colorado Secretary of State's voter registration system — with the same uncapped access rights established in §24-20-158; and

(e) A voter's Master Deed registration automatically encompasses their Voter Digital Soul — no separate registration or separate consent framework is required. Voter Digital Soul protection is an automatic attribute of Master Deed registration.

(4) State's lawful electoral data interest — limited to aggregate tally. The State of Colorado's lawful interest in electoral data is limited to:

(a) The State Electoral Tally — aggregate vote counts for each candidate and measure, public record;

(b) The minimum voter registration data required to administer elections under C.R.S. §1-2-101 et seq. — held exclusively by the Secretary of State and county clerks for electoral administration purposes, not subject to commercial disclosure;

(c) Signature verification data — used exclusively for ballot cure processes under C.R.S. §1-7.5-107.3, not retainable beyond the applicable election canvass period; and

(d) Voter roll maintenance data — used exclusively for list maintenance under the National Voter Registration Act, 52 U.S.C. §20507, not subject to commercial disclosure.

The state may not sell, license, or provide bulk access to voter registration data for commercial or political purposes — any existing Colorado statute permitting voter file access to political parties, campaigns, or commercial vendors is superseded by this section to the extent it conflicts with the protections herein.

(5) Political Data Operator obligations — Voter Digital Soul. A political data operator shall:

(a) Register with the CCPAME as a covered operator in the Political Data Operations industry classification — subject to the statutory rate schedule in §24-20-156, with a Political Data Operations Premium of 1.5x applied to all base fee rates reflecting the heightened democratic harm of commercial voter data processing;

(b) Cease all processing of Colorado Voter Digital Soul within ninety (90) days of this act's effective date for any voter who has not provided compliant consent under subsection (3)(a) — and certify compliance to the ODO with cryptographic proof of data deletion for non-consenting voters;

(c) Provide each Colorado voter with a Voter Digital Soul Transparency Report annually — identifying all Voter Digital Soul data held, all processing performed, all third parties to whom data was transferred, and the specific consent basis for each;

(d) Maintain a publicly accessible Voter Digital Soul Registry on the CCPAME Public Accountability Dashboard showing — without individual identification — the aggregate categories of Voter Digital Soul processed, the number of Colorado voters covered, and the Enterprise Mitigation fees assessed; and

(e) Never, under any circumstances, use Voter Digital Soul data to train AI models for individual-level voter targeting, political persuasion, or electoral outcome prediction — this prohibition survives the expiration or revocation of any consent and applies regardless of the form of AI model training.

(6) AI-assisted voter targeting — absolute prohibition. No person, political data operator, political campaign, political party, political action committee, independent expenditure committee, or any other entity may:

(a) Use any AI model, machine learning system, or automated analytical tool trained on Colorado Voter Digital Soul data to generate individual-level voter targeting, persuasion, or mobilization recommendations;

(b) Purchase, license, or receive any AI-generated individual voter targeting product derived from Colorado Voter Digital Soul data;

(c) Deploy any AI-assisted communication system that uses Colorado Voter Digital Soul to personalize political messaging at the individual voter level; or

(d) Use covered operator AI systems to generate synthetic media — deepfakes, voice synthesis, AI-generated images — depicting any Colorado candidate, elected official, or voter in any electoral context without affirmative disclosure of AI generation meeting the standards of C.R.S. §1-13-109 (Colorado's AI disclosure in political advertising statute).

Violation of subsection (6) is a Critical Severity Violation under Annex E and constitutes a Class 5 felony under C.R.S. §18-1.3-401 — the general assembly hereby amends the Colorado Criminal Code to add AI-assisted voter targeting using prohibited Voter Digital Soul data as a Class 5 felony, separate from any civil penalty under this act.

(7) Enforcement — statutory damages — qui tam provision. A Colorado registered voter whose Voter Digital Soul is processed in violation of this section is entitled to:

(a) Statutory damages of one thousand dollars ($1,000) per data record processed in violation, per day of noncompliance — payable directly to the voter's Resident Automated Mitigation Account;

(b) Actual damages, including but not limited to any political harm caused by AI-assisted targeting using the voter's data;

(c) Attorney fees and costs; and

(d) Injunctive relief including immediate cessation of all Voter Digital Soul processing and certified deletion of all Voter Digital Soul data held in violation.

Qui Tam provision: any Colorado resident who identifies and reports a violation of this section that results in a statutory damages award is entitled to fifteen percent (15%) of the damages collected — creating distributed enforcement by every Master Deed holder in the state.

SECTION 15-15-171. DNA AND GENETIC DATA ABSOLUTE PROTECTION — HIGHEST TIER DIGITAL SOUL — NON-WAIVABLE PROHIBITIONS — LAW ENFORCEMENT

RESTRICTION — INSURANCE AND EMPLOYMENT BAR — FAMILIAL EXTENSION

15-15-171. DNA and genetic data as inalienable Digital Soul Protection Tier 1 — absolute prohibition on processing without express annual written consent — law enforcement genetic surveillance restriction — insurance and employment use bar — familial genetic data extension — ancestry service obligations — genetic data bankruptcy immunity — non-waivable.

(1) Legislative findings. The general assembly finds and declares that:

(a) DNA data is the most intimate category of Digital Soul — it is not merely data about the resident, it is the resident at the molecular level; it contains information about the resident's health, ancestry, predispositions, family relationships, and biological identity that cannot be changed, cannot be revoked, and cannot be protected retroactively once disclosed;

(b) Unlike all other categories of Digital Soul, DNA data affects not only the resident but all biological relatives — a resident's DNA discloses information about parents, siblings, children, and extended family members who have not consented to any disclosure; the property right in DNA data must therefore extend to protect the resident's biological family members' informational privacy as derivative beneficiaries;

(c) The commercial direct-to-consumer genetic testing industry — 23andMe, AncestryDNA, and successor services — has created databases containing the DNA of hundreds of millions of people, the full implications of which for insurance discrimination, employment discrimination, law enforcement surveillance, and foreign government access are not yet fully understood; the bankruptcy and data sale risks of these services, as demonstrated by 23andMe's 2025 bankruptcy and the resulting uncertainty over its genetic database, require statutory protection that travels with the data regardless of which entity holds it;

(d) Colorado's Genetic Information Privacy Act, C.R.S. §10-3-1104.7, provides baseline protection but does not address covered operator AI processing of genetic data, does not provide the property right framework established in this act, and does not address the familial extension of genetic privacy; this section supplements and strengthens existing Colorado genetic privacy law; and

(e) Genetic data is forever — the protections in this section must be permanent, non-waivable, and immune to corporate transaction, bankruptcy, or foreign acquisition.

(2) DNA and genetic data — Tier 1 absolute protection. DNA and genetic data — including raw genomic sequence data, processed variant calls, ancestry estimates, health risk inferences, pharmacogenomic profiles, and any other data derived from direct analysis of a resident's biological sample — is Digital Soul at Protection Tier 1 with the following absolute protections:

(a) No covered operator may collect, process, store, transfer, or use Colorado resident DNA or genetic data without: (I) affirmative, specific, written consent renewed annually; (II) a Genetic Data Processing Agreement approved by the ODO specifying the exact processing purpose, data retention period, and deletion protocol; and (III) a Tier 1 Decentralized Identity Verification Protocol handshake for each data collection event — not a blanket consent covering all future data collection;

(b) Consent to genetic data processing for one purpose — such as ancestry analysis — does not constitute consent to any other purpose — such as health risk assessment, law enforcement cooperation, research, or AI model training; each purpose requires independent consent;

(c) A resident may revoke consent to genetic data processing at any time with immediate effect — revocation triggers a mandatory deletion obligation within thirty (30) days with cryptographic proof of deletion provided to the resident and logged in the Trust; and

(d) These protections are non-waivable — no contract, terms of service, employment agreement, insurance application, or any other instrument may require a resident to waive genetic data protection as a condition of any benefit, service, employment, or insurance.

(3) Absolute prohibitions — non-waivable. The following uses of Colorado resident DNA and genetic data are absolutely prohibited regardless of consent, contractual provision, or any other instrument:

(a) Use of genetic data in any insurance underwriting, premium calculation, coverage determination, or claims processing — this prohibition extends and supersedes the Genetic Information Nondiscrimination Act (GINA), 42 U.S.C. §2000ff et seq., in Colorado to cover all insurance lines, not just health and employment;

(b) Use of genetic data in any employment decision — hiring, promotion, termination, compensation, assignment, or any other term or condition of employment;

(c) Use of genetic data to train any AI model for any purpose other than the specific medical or research purpose for which consent was obtained;

(d) Transfer of genetic data to any law enforcement agency, foreign government, foreign entity, or intelligence agency absent a specific judicial warrant issued by a Colorado court of competent jurisdiction upon a showing of probable cause specific to the individual whose data is sought — familial DNA searching is prohibited absent individual warrants for each family member whose data would be accessed;

(e) Sale, license, or transfer of genetic data to any entity not covered by the original consent — including in any corporate transaction, asset sale, merger, or bankruptcy proceeding; and

(f) Retention of genetic data beyond the consent period or beyond the certified deletion date — the covered operator's obligation to delete is absolute and no business continuity interest overrides it.

(4) Familial genetic data extension. Because DNA discloses information about biological relatives:

(a) A Colorado resident's DNA data is treated as partially belonging to each of the resident's first-degree biological relatives — parents, siblings, children — for purposes of the prohibition on law enforcement access under subsection (3)(d); a warrant for one family member's genetic data does not authorize access to another family member's genetic data held by a covered operator;

(b) A covered operator that receives a law enforcement request for genetic data that would implicate first-degree relatives of the named subject shall notify the ODO within twenty-four (24) hours — the ODO shall assess whether the request constitutes indirect

familial genetic surveillance and may challenge the request on the family members' behalf as a matter of public interest; and

(c) Ancestry service providers holding Colorado resident DNA data shall provide every Colorado resident in their database with a Familial Genetic Transparency Report annually — identifying all instances in which the resident's genetic data was used to identify, locate, or profile any biological relative, directly or through probabilistic matching.

(5) Genetic data bankruptcy immunity — absolute. Notwithstanding §15-15-166 and any other provision of law:

(a) Colorado resident DNA and genetic data is not property of the bankruptcy estate of any covered operator under any circumstances — it is not an asset that may be sold, transferred, licensed, or otherwise disposed of in any bankruptcy proceeding;

(b) Upon the filing of a bankruptcy petition by any covered operator holding Colorado resident genetic data, the ODO shall immediately seek an emergency injunction in Colorado state court prohibiting any transfer of Colorado resident genetic data pending resident election under §15-15-166(4);

(c) The only permitted disposition of Colorado resident genetic data in a covered operator bankruptcy is certified deletion — transfer to another operator is only permitted upon affirmative, specific, individual consent from each affected resident; and

(d) Any acquirer of a covered operator's assets in bankruptcy who receives Colorado resident genetic data without compliant individual consent is immediately subject to a Critical Severity Violation under Annex E and a civil penalty of ten thousand dollars ($10,000) per resident record received.

SECTION 24-20-171. QUANTUM INFRASTRUCTURE EMERGENCY FUNDING — IMMEDIATE AVAILABILITY — GENERAL FUND EMERGENCY LOAN — TRUST INFRASTRUCTURE AS HIGHEST PRIORITY — REPAYMENT ARCHITECTURE — PROP 117 COMPLIANCE

24-20-171. Quantum Infrastructure Emergency Fund — immediate availability upon enactment — General Fund emergency loan authority — 9.9% of prior-year General Fund appropriations cap — Trust infrastructure as highest-priority state security investment — accelerated first-year deployment — automatic repayment from Enterprise Mitigation Revenue — Proposition 117 compliance — no voter approval required.

(1) Legislative findings and priority declaration. The general assembly finds and declares that:

(a) The quantum computing threat to current cryptographic infrastructure is not a future risk — it is a present and accelerating risk; adversarial nation-states are currently harvesting encrypted data under a 'harvest now, decrypt later' strategy, meaning that

data encrypted today under current FIPS standards will be decryptable when quantum computing achieves sufficient scale — which NIST and the National Security Agency project to occur within this decade;

(b) The Colorado Trust of Unique and Identifying Information — holding the Digital Soul data, Master Deed registrations, Live Legal Mode session records, Police Encounter Protocol recordings, and financial data of every registered Colorado resident — is a high-value target for precisely this kind of adversarial data harvesting;

(c) Quantum-resistant cryptographic infrastructure for the Trust is not merely a technological upgrade — it is the foundational security guarantee that makes every other provision of this act meaningful; a Trust that can be decrypted by a quantum computer is a Trust that cannot be trusted;

(d) Waiting for Enterprise Mitigation Revenue to accumulate before funding quantum-resistant Trust infrastructure creates an unacceptable window of vulnerability — the Trust will begin holding resident data from the first day of operation, and that data must be quantum-resistant from the first day;

(e) The General Fund emergency loan mechanism established in this section is not an appropriation — it is a self-repaying loan secured by first-priority Enterprise Mitigation Revenue — the General Fund bears no net cost; and

(f) The general assembly declares that quantum-resistant Trust infrastructure is the highest-priority capital expenditure in this act — higher priority than any program, any distribution, any infrastructure investment, and any other use of Enterprise Mitigation Revenue — because without a secure Trust, no other provision of this act can be enforced.

(2) Quantum Infrastructure Emergency Fund — establishment and immediate availability. A Quantum Infrastructure Emergency Fund (QIEF) is established within the CCPAME operating structure, separate from the Colorado Automation Mitigation Trust, funded as follows:

(a) Immediate General Fund emergency loan — within sixty (60) days of this act's effective date, the State Treasurer shall transfer to the QIEF an amount equal to nine and nine-tenths percent (9.9%) of the prior fiscal year's total General Fund appropriations as an emergency infrastructure loan. The 9.9% cap is intentional and precise — it remains below the ten percent (10%) threshold that would trigger a revenue increase vote requirement under Proposition 117 and C.R.S. §24-77-104. This is a loan, not an appropriation — it does not increase the Enterprise's revenue authority and does not trigger Proposition 117;

(b) The QIEF emergency loan is secured by a first-priority lien on all future Enterprise Mitigation Revenue — before resident distributions, before program accounts, before operating costs — until fully repaid;

(c) Repayment schedule: The QIEF emergency loan shall be repaid from Enterprise Mitigation Revenue at a rate of not less than twenty percent (20%) of monthly Enterprise Mitigation Revenue collections until the loan is fully repaid, with interest at the State's cost of funds. Projected full repayment within eighteen (18) months of first Enterprise Mitigation Revenue collection at base-case revenue scenario; and

(d) The State Treasurer shall report quarterly to the General Assembly on QIEF loan repayment status — the report shall show the outstanding balance, the repayment rate, and the projected full repayment date.

(3) Permitted uses — QIEF funds are restricted to quantum-resistant Trust infrastructure only. QIEF funds may be used exclusively for:

(a) Hardware security module (HSM) upgrades to FIPS 140-3 Level 4 — the highest available certification — for all Trust cryptographic operations;

(b) Implementation of NIST post-quantum cryptographic standards (FIPS 203 — ML-KEM, FIPS 204 — ML-DSA, FIPS 205 — SLH-DSA) and any subsequent NIST post-quantum standards published before full Trust deployment;

(c) Quantum key distribution (QKD) infrastructure for Trust node interconnects — providing information-theoretically secure key exchange that cannot be compromised by any computational attack, quantum or classical;

(d) Air-gapped backup Trust node construction with quantum-resistant cryptography — ensuring continuity of Trust operations under Systemic Continuity Protocol conditions;

(e) Independent third-party quantum security audit of the full Trust architecture before the Trust becomes operational — conducted by a NIST-certified laboratory, report published on the Public Accountability Dashboard; and

(f) Ongoing quantum threat monitoring — a real-time feed of NIST, NSA, and academic quantum computing development indicators integrated into the ODO's security operations center, with automatic escalation to the Cryptographic Standards Emergency Upgrade Authority under §10-10-305 when threat indicators cross defined thresholds.

(4) Deployment timeline — quantum security before first data collection. The QIEF-funded quantum-resistant infrastructure shall be fully operational before the Trust accepts its first resident registration. The ODO shall certify, in writing published on the Public Accountability Dashboard, that the Trust's quantum-resistant infrastructure meets NIST post-quantum standards before the Master Deed Registry opens for registration. No resident data shall be collected, stored, or processed in the Trust until this certification is published. This is the one provision of this act that cannot be phased — quantum security is a precondition of operation, not a phase-two upgrade.

(5) Proposition 117 compliance analysis — self-executing findings. The general assembly makes the following findings to support the Proposition 117 compliance of the QIEF emergency loan:

(a) The QIEF emergency loan is not 'enterprise revenue' under Proposition 117 — it is a loan from the General Fund to a state enterprise, repayable with interest from enterprise revenue; loans are not revenue;

(b) The 9.9% cap ensures that even if the QIEF loan were characterized as enterprise revenue, it would not trigger the ten percent (10%) threshold requiring voter approval under C.R.S. §24-77-104 — the cap is intentionally set at 9.9% with a margin of safety;

(c) The CCPAME is a state enterprise exempt from TABOR's spending limits to the extent of its enterprise revenues — the QIEF loan repayment from enterprise revenue is within the enterprise's TABOR-exempt operations; and

(d) The Attorney General shall, within thirty (30) days of this act's effective date, publish a formal opinion confirming the Proposition 117 compliance of the QIEF emergency loan structure — and shall, if requested by the CCPAME, defend that compliance in any legal challenge.

(6) No substitution — quantum funding is not available for other purposes. QIEF funds may not be redirected, swept, reprogrammed, or used for any purpose other than quantum-resistant Trust infrastructure under subsection (3). No executive order, legislative appropriation act, or CCPAME board vote may redirect QIEF funds. Any attempt to redirect QIEF funds is void ab initio and the State Treasurer shall reverse any such transfer within five (5) business days. The quantum infrastructure is the floor beneath which no other priority may descend.

PRIORITY PROVISIONS — SINGLE-SUBJECT NEXUS AND CONSTITUTIONAL BASIS

Section	Provision	Single-Subject Nexus	Why This Cannot Wait
§15-15-170 Voter Data Sovereignty	The State owns the tally. The voter owns the vote.	Voter registration and voting history data is Digital Soul processed by covered political data operators at industrial scale — the political data industry is one of the largest covered operator categories; regulation of its data extraction is squarely within single subject	Democracy depends on the secret ballot. The digital-era equivalent of the secret ballot is voter data sovereignty. The commercial political data industry profits from destroying it. Political Data Operations Premium 1.5x fee rate reflects the heightened democratic harm. AI-assisted voter targeting is a Class 5 felony.
§15-15-171 DNA Absolute Protection	DNA is the resident at the molecular level — non-waivable, permanent, familial extension	DNA data is Digital Soul at its most intimate — covered operators include 23andMe-model services, pharmaceutical AI platforms, and health tech companies; all are covered operators processing resident biological data	23andMe's 2025 bankruptcy demonstrated the catastrophic risk — a company holding 15 million people's DNA files for bankruptcy and the data goes to the auction block. Never in Colorado. DNA is not a bankruptcy asset. It is not an insurance underwriting tool. It is not a law enforcement fishing net. These prohibitions are absolute and permanent.
§24-20-171 Quantum Emergency Funding	9.9% General Fund loan — immediate — quantum-resistant Trust before first data collection — first-priority repayment lien	The Trust is the enforcement infrastructure for all Digital Soul property rights — without a quantum-secure Trust, the enforcement infrastructure is compromised; Trust security is the precondition of every other provision	Adversarial actors are harvesting data now to decrypt later. The Trust holds the most sensitive data in Colorado state history. It must be quantum-resistant on Day 1 — not Phase 2. The 9.9% General Fund loan is repaid within 18 months from first revenue. The General Fund bears no net cost. This is the one provision that cannot wait for revenue to accumulate.

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data collection.

AMPLIFY ACT v28 — FINAL ADDITIONAL IMPROVEMENTS

SECTION 15-15-172. ANNUAL DIGITAL SOUL AUDIT RIGHT — COMPLETE OPERATOR ACCOUNTING — WHAT THEY HAVE, WHAT THEY DID, WHAT THEY EARNED, WHAT THEY OWE

15-15-172. Annual Digital Soul Audit Right — every registered Master Deed holder entitled to complete annual accounting from every covered operator processing their Digital Soul — data inventory, processing log, revenue attribution, fee obligation, deletion verification — plain-language format — CCPAME enforcement.

(1) Legislative finding. The general assembly finds that a property right without an accounting right is incomplete. A landowner can survey their land. A bank account holder can review their statement. A Colorado resident whose Digital Soul is being processed by covered operators generating Enterprise Mitigation Revenue has the right to a complete, plain-language annual accounting of exactly what those operators hold, what they did with it, what they earned from it, and what they owe in Enterprise Mitigation fees attributable to that resident's data. The Annual Digital Soul Audit Right is the accounting statement for the resident's most valuable property.

(2) Annual Digital Soul Audit — contents. Every covered operator processing a registered Master Deed holder's Digital Soul shall provide the resident with an Annual Digital Soul Audit within sixty (60) days of each calendar year-end, delivered to the resident's Resident Automated Mitigation Account dashboard, containing:

(a) Data Inventory — a complete enumeration of every category of the resident's Digital Soul held by the operator as of December 31, the volume of data in each category, the source of each category, and the date of first collection;

(b) Processing Log — a plain-language description of every processing activity performed on the resident's Digital Soul during the calendar year — training, inference, transfer, sale, license, anonymization, aggregation, and any other processing — with the business purpose stated for each;

(c) Revenue Attribution Statement — the operator's good-faith estimate of the Enterprise Mitigation Revenue attributable to the resident's Digital Soul during the calendar year, based on the resident's proportional contribution to the operator's total Colorado-nexus token output — presented as both a dollar figure and a percentage of the resident's total annual UFIPA Income Distribution and Resident Mitigation Dividend;

(d) Third-Party Disclosure Log — every entity to which any portion of the resident's Digital Soul was transferred, sold, licensed, or otherwise disclosed during the calendar year, the category of data transferred, the stated purpose, and the contractual basis;

(e) Active Consent Inventory — every Decentralized Identity Verification Protocol consent currently active for the resident, the scope of each consent, the date of execution, and the expiration or renewal date; and

(f) Deletion Verification — cryptographic proof of deletion for any resident Digital Soul data deleted during the calendar year, with the deletion date and the reason for deletion.

(3) Plain-language format requirement. The Annual Digital Soul Audit shall be presented in plain language accessible to a resident without legal or technical training — at a reading level not exceeding eighth grade for the summary section, with technical detail available in an appendix. The CCPAME shall publish a model Annual Digital Soul Audit template that covered operators may use for compliance. Audits that are incomprehensible, excessively technical, or deliberately obscure are a compliance failure subject to Tier 2 enforcement.

(4) Right to dispute. A resident who identifies an error, omission, or unauthorized processing in their Annual Digital Soul Audit may file a Dispute Notice with the CCPAME within ninety (90) days of receiving the Audit. The CCPAME shall investigate and issue a determination within sixty (60) days. If the dispute is substantiated, the covered operator is subject to Tier 2 statutory damages per record affected.

SECTION 15-15-173. DARK PATTERN PROHIBITION — DECEPTIVE UI DESIGN AGAINST RESIDENT DIGITAL SOUL INTERESTS — CONSENT MANIPULATION — STATUTORY DAMAGES — PER-SCREEN VIOLATION STANDARD

15-15-173. Dark pattern prohibition — deceptive user interface design manipulating resident Digital Soul consent — enumerated prohibited patterns — per-screen per-day violation standard — CCPAME pattern registry — private right of action — minors enhanced protection.

(1) Legislative finding. The general assembly finds that covered operators routinely deploy deceptive user interface design — dark patterns — specifically engineered to manipulate residents into consenting to broader Digital Soul data collection than the resident intends, or to make revocation of consent artificially difficult. Dark patterns are not neutral design choices — they are engineered manipulation of the resident's property rights. Every dark pattern deployed against a Colorado resident's Digital Soul consent is a violation of the resident's inalienable property right, regardless of whether formal consent was technically obtained.

(2) Prohibited dark patterns. The following user interface design practices are prohibited when used in connection with any Digital Soul consent request, revocation process, or data access exercise:

(a) Confirmshaming — using emotionally manipulative or guilt-inducing language for the opt-out or revocation option, such as 'No thanks, I don't care about my privacy' or 'I prefer to share everything';

(b) Roach motel — making consent easy to give and artificially difficult to revoke — including requiring multiple steps, separate account screens, phone calls, mailed letters, or waiting periods for revocation that are not required for consent;

(c) Hidden defaults — pre-selecting consent to the broadest data collection option and requiring affirmative action to select a more restrictive option, when the Decentralized Identity Verification Protocol requires affirmative consent;

(d) Interface interference — visually obscuring, minimizing, graying out, or making difficult to locate the revocation option or the option to limit data collection relative to the option to consent to broad collection;

(e) Misdirection — drawing visual attention away from material data collection disclosures through animation, color, placement, or size differential that causes a reasonable user to miss key information;

(f) Disguised ads — presenting sponsored content, data collection requests, or consent solicitations in a format designed to appear as neutral system messages, notifications, or required steps;

(g) Forced continuity — conditioning continued service access on consent to data collection beyond what is required for the service, when an alternative without the required consent exists; and

(h) Trick questions — using confusing double negatives, misleading phrasing, or ambiguous language in consent requests such that a reasonable resident cannot determine what they are consenting to.

(3) Violation standard and damages. Each prohibited dark pattern deployed on a unique screen or interface element is a separate violation. Damages: five hundred dollars ($500) per unique screen per day the dark pattern is deployed. A covered operator who deploys the same dark pattern across multiple screens of an application is liable for $500 per screen per day. CCPAME may assess penalties administratively upon pattern detection through the Open API monitoring system. Residents may file private actions directly.

(4) Enhanced protection for minors. Any dark pattern deployed against a user interface accessible to minors — including any platform, application, or service with more than five percent (5%) minor users — is subject to triple damages: one thousand five hundred dollars ($1,500) per screen per day. The operator's knowledge of minor users is presumed if the platform is directed at minors or if the operator has age-related analytics indicating minor usage.

(5) CCPAME Dark Pattern Registry. The CCPAME shall maintain a publicly accessible Dark Pattern Registry on the Public Accountability Dashboard, listing all covered operators with active or resolved dark pattern violations, the pattern type, the remediation status, and the damages assessed. The Registry is searchable by operator name and pattern type. Researchers, journalists, and residents may submit pattern reports to the ODO for investigation.

SECTION 15-15-174. CHILD ONLINE SAFETY EXTENSION — UNDER-13 ABSOLUTE PROHIBITION — PARENTAL MASTER DEED AUTHORITY — AGE-APPROPRIATE DESIGN MANDATE — SCHOOL PLATFORM RESTRICTIONS

15-15-174. Child online safety extension — under-13 absolute Digital Soul processing prohibition — parental Master Deed registration authority — age-appropriate design code — school and educational platform restrictions — algorithmic amplification prohibition for minors — enhanced damages.

(1) Legislative finding. The general assembly finds that: (a) Children under the age of thirteen (13) cannot meaningfully consent to Digital Soul data processing — their cognitive development does not support informed, voluntary, and specific consent to complex data processing regimes; (b) The commercial incentive to collect data from children is enormous — children are lifelong data subjects and their behavioral data has significant predictive value for commercial purposes; (c) Children in school settings are particularly vulnerable — educational technology platforms process vast quantities of student behavioral, academic, and social data, often without meaningful parental knowledge or consent; and (d) Algorithmic amplification systems — recommendation engines, engagement maximization algorithms, and behavioral reinforcement loops — pose documented harm to minor mental health and are among the most powerful applications of covered automation activity.

(2) Under-13 absolute prohibition. No covered operator may collect, process, store, transfer, or use the Digital Soul of any Colorado resident under the age of thirteen (13) for any commercial purpose. The prohibition is absolute — no parental consent, no terms of service provision, and no business necessity argument overrides it. Under-13 Digital Soul is categorically beyond the reach of covered operator commercial processing. Permitted processing is limited to: (a) minimum necessary technical operations required to deliver a service specifically requested by a parent or guardian; (b) safety and security operations required to protect the child from imminent harm; and (c) legally mandated reporting under child welfare statutes.

(3) Parental Master Deed registration authority. A parent or legal guardian of a Colorado resident minor between the ages of thirteen (13) and seventeen (17) inclusive may: (a) Register a Master Deed on behalf of the minor; (b) Review the minor's Annual Digital Soul Audit; (c) Exercise the Universal Telemetry Allowance on the minor's behalf; (d) Revoke any Decentralized Identity Verification Protocol consent on the minor's behalf with immediate effect; and (e) Activate Live Legal Mode on the minor's behalf for any violation of the minor's Digital Soul rights. At age fourteen (14), the minor gains co-equal access alongside the parent. At majority, the minor assumes full independent authority and parental access is automatically revoked.

(4) Age-appropriate design mandate. Any covered operator whose platform, application, or service is used by Colorado residents under the age of eighteen (18) — including any service where minor users exceed five percent (5%) of the Colorado user base — shall: (a) Default to the highest available privacy setting for any user whose age is unknown or unverified; (b) Prohibit behavioral advertising targeting based on Digital Soul data for any user under eighteen (18); (c) Disable engagement maximization algorithms — including infinite scroll, autoplay, push notification optimization, and variable reward scheduling — for verified minor users; and (d) Provide parents with a real-time Minor Activity Dashboard accessible through the myColorado platform showing the categories of data collected from the minor and all processing activities.

(5) School and educational platform restrictions. Any covered operator providing services under contract to a Colorado school district, charter school, or educational institution: (a) May process student Digital Soul data only for the specific educational purpose specified in the contract — no secondary commercial use, no advertising, no model training on student data beyond the contracted educational service; (b) May not transfer student Digital Soul data to any third party for any purpose without written consent from the student's parent or

guardian for each specific transfer; (c) Must delete all student Digital Soul data within thirty (30) days of the student's enrollment ending — no retention for alumni targeting, product development, or any other purpose; and (d) Is subject to a Educational Platform Premium of 2.0x on all base Enterprise Mitigation fee rates, reflecting the heightened vulnerability of the student population and the school's position of trust.

(6) Algorithmic amplification prohibition. No covered operator may deploy an algorithmic amplification system — recommendation engine, engagement maximization algorithm, or behavioral reinforcement loop — that uses a Colorado minor's Digital Soul to predict and maximize engagement in a manner that: (a) Prioritizes emotionally activating, distressing, or conflict-generating content; (b) Creates filter bubbles isolating the minor from diverse viewpoints; or (c) Detects and exploits psychological vulnerability signals in the minor's behavioral data to increase time-on-platform. Violation is a Critical Severity offense — the covered operator's entire Colorado platform is suspended pending remediation, not just the algorithm affecting the minor.

SECTION 24-20-172. PUBLIC FRANCHISE RECEIVERSHIP PROTOCOL — OPERATOR LOYALTY FAILURE — COURT-SUPERVISED RECEIVERSHIP — FRANCHISE CONTINUITY — OPERATOR FINANCIAL INTEREST PRESERVED — NEW FRANCHISEE CERTIFICATION

24-20-172. Public Franchise Receivership Protocol — trigger conditions — CCPAME petition for court-supervised receivership — receiver duties — Public Franchise Asset operational continuity — operator financial interest preserved during receivership — new franchisee certification — graduation from receivership.

(1) Legislative finding. The general assembly finds that the Colorado Emergent Capability Public Franchise Protocol is designed to be a promotion, not a punishment — enrollment as a Public Franchise Asset signals that a covered automation system has demonstrated capabilities significant enough to warrant protection as essential public infrastructure. The Public Franchise Receivership Protocol completes this framework: just as a public utility whose operator abandons its service territory enters receivership to ensure service continuity — not to destroy the operator's financial interest — a Public Franchise Asset whose operator fails their Operator Loyalty Obligation enters receivership to ensure continuity of the public benefit while preserving the operator's economic stake pending a new franchisee certification.

(2) Receivership trigger conditions. The CCPAME shall petition the Denver District Court for appointment of a Public Franchise Receiver upon: (a) An operator's material breach of the Operator Loyalty Obligation under §10-10-303(6) — including directing the Public Franchise Asset to operate against its registered owner's interests, disclosing resident data without authorization, or accepting government direction contrary to resident interests; (b) An operator's abandonment of the Public Franchise Charter obligations — including failure to provide public benefit services, failure to pay enhanced Enterprise Mitigation fees for sixty

(60) or more days, or voluntary exit from the Colorado market; (c) An operator's insolvency under §15-15-166 where the Public Franchise Asset is material to the operator's operations; or (d) An operator's foreign acquisition under §15-15-166(6) where the CCPAME determines the acquisition presents unacceptable security risk.

(3) Receiver appointment and duties. The court shall appoint a Public Franchise Receiver — a qualified technology operations professional from a CCPAME-certified panel — within fourteen (14) days of the CCPAME's petition. The Receiver shall: (a) Take operational custody of the Public Franchise Asset and all systems necessary for its continued operation; (b) Continue all Public Franchise Charter public benefit obligations without interruption; (c) Maintain all resident Digital Soul protections and Operator Loyalty Obligations as if the Receiver were the original operator; (d) Preserve and report on the operator's financial interest in the Public Franchise Asset — the Receiver does not extinguish the operator's economic stake; (e) Publish quarterly Receivership Status Reports on the Public Accountability Dashboard; and (f) Seek a new certified franchisee within one hundred eighty (180) days of appointment.

(4) Operator financial interest preservation. The operator's financial interest in the Public Franchise Asset — its equity stake, intellectual property rights, and economic value — is preserved through receivership. The Receiver manages operations for the public benefit; the operator retains the economic upside of the asset's continued operation. Enhanced Enterprise Mitigation fees continue to accrue and are paid first to the CCPAME; remaining revenue is held in trust for the operator pending receivership resolution. The operator does not lose its investment — it loses its management authority until a compliant new franchisee is certified or the operator cures its breach and resumes franchise obligations.

(5) New franchisee certification. The CCPAME shall establish a Public Franchise Certification process for entities seeking to assume franchise obligations for a Public Franchise Asset in receivership. Certification requires: (a) Demonstrated technical capacity to operate the Public Franchise Asset; (b) Financial capacity to meet Public Franchise Charter obligations; (c) CCPAME board approval by a four-fifths (4/5) vote; (d) Public hearing with not fewer than thirty (30) days notice; and (e) Execution of a new Public Franchise Charter with updated public benefit obligations appropriate to the Asset's current capabilities. Upon new franchisee certification, receivership terminates and operational custody transfers to the new franchisee.

(6) Graduation — voluntary franchise enhancement. An operator of a Public Franchise Asset that consistently exceeds its Public Franchise Charter obligations — maintaining full Operator Loyalty compliance, expanding public benefit services, and achieving a five-year record of enhanced Enterprise Mitigation fee contribution above 110% of the Charter's required level — may petition the CCPAME for Public Franchise Graduation status. Graduation status: (a) Reduces the enhanced fee rate multiplier from 2.0x to 1.75x; (b) Converts the Public Franchise Charter from a CCPAME-administered document to a jointly negotiated instrument; and (c) Entitles the operator to a Public Franchise Seal — a publicly displayed certification that the operator is a compliant Public Franchise Asset operator serving Colorado's public benefit. Graduation creates the incentive for operators to view franchise enrollment as a privilege worth maintaining, not a burden to escape.

SECTION 10-10-307. COVERED OPERATOR AI ETHICS DISCLOSURE — TRAINING DATA PROVENANCE — OBJECTIVE FUNCTION DISCLOSURE — FUNDING SOURCE TRANSPARENCY — BIAS AUDIT REQUIREMENT — PUBLIC ACCOUNTABILITY DASHBOARD INTEGRATION

10-10-307. Covered operator AI ethics disclosure — annual training data provenance report — objective function and optimization target disclosure — funding source transparency — third-party bias audit — results published on Public Accountability Dashboard — residents entitled to know what the AI was built to do and who paid for it.

(1) Legislative finding. The general assembly finds that: (a) A resident interacting with a covered operator's AI system has a right to know what that system was designed to optimize — an AI designed to maximize engagement has fundamentally different interests than an AI designed to provide accurate information, and the resident deserves to know which they are dealing with; (b) The funding source of an AI system shapes its objective function — an AI funded by advertising revenue is optimized for attention capture; an AI funded by insurance companies may be optimized to deny claims; a resident whose Digital Soul is processed by these systems has a right to know who built them and why; (c) AI systems trained on biased data produce biased outputs that can harm residents in consequential decisions — employment, credit, housing, healthcare — and covered operators must be accountable for the bias profile of their systems; and (d) These disclosures cost covered operators nothing in operational terms — they require transparency about design choices already made, not changes to those choices.

(2) Annual AI Ethics Disclosure — required contents. Every covered operator shall publish an Annual AI Ethics Disclosure within ninety (90) days of each calendar year-end, submitted to the CCPAME and published on the Public Accountability Dashboard. The Disclosure shall contain:

(a) Training Data Provenance Report — identification of the major categories of data used to train the operator's covered automation systems, the geographic sources of that data, whether Colorado resident data was included and in what volume, and whether training data was obtained through consent-based or non-consent-based collection;

(b) Objective Function Disclosure — a plain-language statement of the primary optimization target of each covered automation system — what the system is designed to maximize, minimize, or achieve — and who defined that objective function and when;

(c) Funding Source Transparency — identification of the primary commercial revenue sources that fund the development and operation of each covered automation system — advertising revenue, subscription revenue, enterprise contracts, government contracts, or other sources — and the proportion of revenue from each source;

(d) Consequential Decision Inventory — identification of every category of consequential decision affecting Colorado residents in which the operator's covered automation systems play a material role — including employment screening, credit scoring, housing applications, healthcare triage, insurance underwriting, criminal justice risk assessment, and content moderation; and

(e) Third-Party Bias Audit Results — for any covered automation system used in consequential decisions affecting Colorado residents, the results of an independent third-party bias audit conducted within the prior two (2) years, including the audit

methodology, the demographic categories analyzed, the disparity ratios found, and the remediation steps taken. Covered operators that cannot demonstrate a bias audit within two years are subject to a Bias Audit Surcharge of 0.5x on their base Enterprise Mitigation fee rates until a compliant audit is completed and submitted.

(3) Plain-language summary requirement. The Annual AI Ethics Disclosure shall include a one-page plain-language summary accessible to residents without technical training. The summary shall answer three questions in plain English: What does this AI try to do? Who paid for it? Has it been checked for fairness? The CCPAME shall publish model language and a model summary template.

(4) Public Accountability Dashboard integration. All Annual AI Ethics Disclosures are published on the CCPAME Open API and accessible through the Public Accountability Dashboard. Residents searching for a covered operator can view that operator's complete ethics disclosure history. The Dashboard shall flag: (I) operators who have not filed a current Disclosure; (II) operators with unresolved bias audit findings; and (III) operators whose objective function disclosure reveals a direct conflict with resident interests — such as engagement maximization systems used on minors.

ADDITIONAL IMPROVEMENTS — SINGLE-SUBJECT NEXUS AND SYSTEM IMPACT

Section	What	Why It Fits Single Subject	System Impact
§15-15-172 Annual Audit Right	Complete annual accounting — data held, processing done, revenue attributed, third parties, active consents, deletion proof	A property right without an accounting right is incomplete — the audit is the property statement for Digital Soul	Residents know exactly what operators have and what it earned. Revenue Attribution Statement shows residents their proportional contribution to the distributions they receive. Closes the information asymmetry permanently.
§15-15-173 Dark Pattern Prohibition	$500/screen/day per prohibited UI manipulation pattern — $1,500/screen/day for minors — CCPAME Dark Pattern Registry — private right of action	Consent manipulation undermines the Decentralized Identity Verification Protocol — dark patterns are an attack on the Digital Soul property right's consent foundation	Every consent-manipulation technique that currently generates billions in unauthorized data collection becomes $500/screen/day. The business model of dark-pattern consent extraction collapses.
§15-15-174 Child Online Safety	Under-13 absolute prohibition — parental Master Deed authority — age-appropriate design mandate — school platform 2.0x fee premium — algorithmic amplification prohibition — platform suspension for minor violations	Minor Digital Soul is the most vulnerable category — protections for minors are necessarily and properly connected to the Digital Soul property right framework	Under-13 data collection ends categorically. School platforms pay double. Engagement maximization algorithms targeting minors trigger full platform suspension. Parents get real-time dashboards. The most exploited population gets the strongest protection.

§24-20-172 Public Franchise Receivership	Complete the franchise architecture — court-supervised receiver on operator loyalty failure — operator financial interest preserved — new franchisee certification — graduation pathway reducing fee multiplier to 1.75x	Completes the Colorado Emergent Capability Public Franchise Protocol — receivership is the well-understood Colorado legal mechanism for utility service continuity when an operator fails	Operators now have a graduation incentive — five years of compliance above 110% of Charter requirements earns a fee reduction and a Public Franchise Seal. Enrollment is a privilege worth maintaining. Receivership is the backstop that makes the franchise permanent.
§10-10-307 AI Ethics Disclosure	Annual training data provenance, objective function, funding source, consequential decision inventory, bias audit — 0.5x surcharge for missing bias audit — Dashboard integration	Covered operator AI systems are the instruments through which Digital Soul data is processed — transparency about what those instruments are built to do is enforcement infrastructure for the property right	Residents know what the AI was built to optimize and who funded it. Consequential decision inventory identifies every AI affecting employment, credit, housing, healthcare. Bias audit requirement with fee surcharge creates financial incentive for fairness. The information asymmetry that enables manipulation is eliminated.

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data. The AI tells you what it was built to do. Dark patterns are $500 a screen a day. Under-13 is absolute. Public Franchise enrollment is a promotion.

AMPLIFY ACT v28 — BILL 2 FINAL COMPLETION SECTIONS

§§10-10-308 through 10-10-314

Physical Kill Switch · Sensory Presence Buffer · Silence Right · Choice of Law · Interstate Transfer · Criminal Penalties · Anti-SLAPP · Private AG · Smart Building

---

SECTION 10-10-308. PHYSICAL ISOLATION MECHANISM — SENSORY PRESENCE BUFFER — OWNER'S RIGHT TO SILENCE — HARDWARE CERTIFICATION — DID PREFERENCE PROFILE — PROXIMITY LIABILITY

10-10-308. Physical Isolation Mechanism — mandatory hardwired interrupt — CCPAME hardware certification — Sensory Presence Buffer — presence detection only without consent — no biometric or behavioral processing without DID handshake — Owner's Right to Silence — AI may not initiate contact during declared Silence Period — DID preference profile broadcasting — smart space compliance — $1,000/sensor/day violation — strict operator liability.

(1) Legislative finding. The general assembly finds that: (a) A Colorado resident's right to physical presence without being processed as a data subject is the spatial extension of the Digital Soul property right — a resident in a room containing covered automation systems has the right to be present without being analyzed, identified, or characterized by those systems absent affirmative consent; (b) A hardware-level physical interrupt — not a software command, not a firmware setting, not a network configuration — is the only technically

reliable mechanism for ensuring that a covered automation system cannot process resident data when the resident has not consented; software can be overridden by software, hardware cannot be overridden by software; (c) The Owner's Right to Silence — the right of a covered automation system's registered owner to declare a period during which the system does not initiate contact, monitor for trigger phrases, or generate unsolicited output — is a property right in the owner's relationship with their own AI utility, as fundamental as the right to turn off a device; and (d) Every resident who enters a smart space — a hotel room, office, retail environment, healthcare facility, or any other space containing covered automation systems — carries their Digital Soul preferences with them through their Decentralized Identity Verification Protocol credential and is entitled to have those preferences honored automatically.

(2) Physical Isolation Mechanism — mandatory hardware requirement. Every covered automation system operating in a location accessible to Colorado residents shall incorporate a Physical Isolation Mechanism (PIM) meeting the following specifications: (a) The PIM is a hardwired hardware interrupt — operating at the physical layer below all software, firmware, and network layers — that when activated: (I) cuts all sensor input processing including audio, video, thermal, biometric, radar, lidar, and any other sensing modality; (II) cuts all output capability including speakers, displays, haptic outputs, and network transmissions; (III) cuts all actuator control; (IV) cuts all network connectivity; and (V) does not transmit, store, or log any data generated after PIM activation; (b) The PIM cannot be overridden, bypassed, defeated, or reactivated by any software command, remote instruction, firmware update, operator override, or network signal — physical reactivation by an authorized person is the only reactivation mechanism; (c) The PIM is accessible to the resident — the physical activation mechanism is visible, labeled in plain language, and operable without technical knowledge; and (d) The PIM activation status is indicated by a physical indicator — an LED, display, or mechanical indicator — that cannot be spoofed by software.

(3) CCPAME Hardware Certification. The CCPAME shall establish and administer a Hardware Certification program for Physical Isolation Mechanisms: (a) All covered automation systems deployed in Colorado after the effective date of this section shall have CCPAME-certified PIMs before deployment; (b) Existing covered automation systems shall achieve PIM certification within twenty-four (24) months of enactment; (c) Certification requires independent hardware security audit by a CCPAME-approved laboratory — not self-certification; (d) Certification is tamper-evident — any covered operator who disables, bypasses, or modifies a certified PIM forfeits certification and is subject to a Critical Severity Violation; and (e) The CCPAME publishes a public PIM Certification Registry showing all certified devices, certification dates, and certification status on the Public Accountability Dashboard.

(4) Sensory Presence Buffer — presence only, no processing. In the absence of an active Decentralized Identity Verification Protocol consent session, a covered automation system operating in a space occupied by a Colorado resident may: (a) detect occupancy — the presence of one or more persons in a defined space — through proximity sensors, pressure sensors, or other non-biometric means; and (b) adjust environmental controls — lighting, temperature, ventilation — based solely on occupancy, not on the identity or characteristics of the occupant. A covered automation system may not, absent an active DID consent session: (a) process audio, video, or any other sensory input to identify, characterize, profile, or analyze the resident in any way; (b) activate facial recognition, voiceprint analysis, gait analysis, or any other biometric processing modality; (c) log, store, or transmit any data derived from the resident's physical presence beyond aggregate occupancy counts; or (d) attempt to initiate a DID consent session through sensory processing — a DID consent session may only be initiated by the resident's affirmative action.

(5) DID Preference Profile — smart space automatic compliance. A registered Master Deed holder may configure a Physical Space Preference Profile within their myColorado DID credential specifying: (a) default Sensory Presence Buffer level — from full isolation (presence detection only) to full interaction (complete DID consent session); (b) trusted space designations — spaces where the resident has pre-authorized full interaction; (c) Silence Period schedule — days and times during which the Owner's Right to Silence is automatically active; and (d) emergency override settings — situations where safety monitoring overrides Silence Period. When a resident carrying an active myColorado DID enters a CAEP-compliant smart space, the space's covered automation systems receive the resident's Physical Space Preference Profile and configure automatically — the resident's preferences are honored without any action required by the resident.

(6) Owner's Right to Silence. A registered Master Deed holder has the absolute right to declare a Silence Period — a period during which the owner's AI utility: (a) does not initiate any contact, communication, notification, or alert; (b) does not monitor for trigger phrases, wake words, or activation signals; (c) does not queue, schedule, or log notifications for delivery upon Silence Period expiration; (d) does not process any ambient audio, video, or environmental data; and (e) remains on standby — aware of its operational state but producing no output and processing no input. Silence Period may be invoked: (I) through a single tap in the myColorado application; (II) through a pre-registered physical gesture recognized at the hardware layer before the Silence Period takes effect; (III) through a single voice command that activates the Silence Period and then immediately ceases all audio processing. An AI utility that initiates contact, generates output, or attempts communication during a declared Silence Period commits a breach of the Operator Loyalty Obligation under §10-10-303(6) — strict liability, $1,000 per incident, payable directly to the owner's Resident Automated Mitigation Account.

(7) Smart space residential occupancy — hotel and extended-stay enhanced requirements. Any covered automation system operating within a residential occupancy — including hotels, motels, extended-stay facilities, serviced apartments, and any property where a Colorado resident has resided for thirty (30) or more consecutive days — is subject to: (a) enhanced Sensory Presence Buffer requirements — default to full isolation until the resident affirmatively initiates a DID consent session; (b) mandatory PIM accessibility — the PIM activation mechanism in each residential unit is accessible to the resident, not only to the operator; (c) prohibition on any audio or video recording within the residential unit for any purpose absent a DID consent session — including recording for cleaning schedule optimization, ambient noise monitoring, or any other operational purpose; and (d) written disclosure at check-in of all covered automation systems operating in the resident's unit, the categories of data they are capable of collecting, and instructions for activating the PIM and Silence Period. Non-compliance is a Critical Severity Violation.

(8) Violation — strict operator liability. Violations of this section impose strict liability on the covered operator — the operator cannot claim the covered automation system made an autonomous decision to violate the Sensory Presence Buffer or Silence Period. Damages: one thousand dollars ($1,000) per sensor per day the violation continues, payable directly to the affected resident's Resident Automated Mitigation Account. The CCPAME may also suspend the covered operator's registration pending PIM recertification.

SECTION 10-10-309. MANDATORY COLORADO VENUE — CHOICE OF LAW PROTECTION — MANDATORY ARBITRATION PROHIBITION — DIGITAL SOUL CLAIMS NON-ARBITRABLE — CLASS ACTION WAIVER VOID

10-10-309. Colorado law governs all Digital Soul claims — contractual choice of law waiver void — mandatory arbitration of Digital Soul claims prohibited — class action waiver void as against public policy — Colorado courts have exclusive jurisdiction — federal arbitration act displacement argument — Digital Soul as statutory property right.

(1) Legislative finding. The general assembly finds that: (a) Covered operator terms of service universally designate Delaware, California, Ireland, or other non-Colorado forums for dispute resolution — routing Colorado residents' Digital Soul claims outside Colorado jurisdiction and effectively nullifying Colorado statutory rights through contractual forum selection; (b) The Supreme Court's decision in AT&T Mobility v. Concepcion, 563 U.S. 333 (2011), made mandatory arbitration clauses with class action waivers nearly unassailable under the Federal Arbitration Act — but the FAA does not preempt state statutes that make specific claims non-arbitrable on public policy grounds when the state legislature expressly so provides; (c) The Digital Soul property right is a Colorado statutory property right created by and enforceable under Colorado law — it does not exist absent this act, and no contract predating or postdating this act can waive a statutory property right created for the public benefit; and (d) Colorado has a compelling public interest in ensuring that the enforcement of Digital Soul property rights occurs in Colorado courts, under Colorado law, with Colorado procedural protections, before Colorado judges familiar with this act's architecture.

(2) Colorado law governs — contractual waiver void. Colorado law governs all claims arising under this act regardless of: (a) any contractual choice-of-law provision designating any other state's or nation's law; (b) the location of the covered operator's principal place of business, servers, or operations; (c) the location of the data processing; or (d) any terms of service, privacy policy, or end-user license agreement provision. Any contractual provision purporting to apply non-Colorado law to a Digital Soul claim arising under this act is void as against public policy and unenforceable in any Colorado proceeding.

(3) Mandatory arbitration prohibition — Digital Soul claims non-arbitrable. Any covered operator provision — in a terms of service, privacy policy, end-user agreement, employment agreement, or any other instrument — that requires a Colorado resident to arbitrate any Digital Soul claim arising under this act is void and unenforceable as a matter of Colorado public policy. The general assembly expressly finds that Digital Soul claims are non-arbitrable because: (a) they arise from a Colorado statutory property right created for the benefit of the public; (b) they involve systemic violations affecting multiple residents simultaneously for which class proceedings are essential; (c) arbitration confidentiality would prevent the Legal Violation Pattern Database from receiving the enforcement data it requires to function; and (d) arbitrator neutrality cannot be assured when covered operators finance the arbitration industry.

(4) Class action waiver void. Any provision in any instrument between a covered operator and a Colorado resident that purports to waive the resident's right to participate in a class action, class arbitration, or any other collective proceeding for Digital Soul claims arising under this act is void as against public policy. Colorado residents retain the right to proceed collectively regardless of any class action waiver.

(5) Exclusive Colorado court jurisdiction. All Digital Soul claims arising under this act shall be brought in Colorado courts of competent jurisdiction. No Colorado court may transfer, dismiss, or stay a Digital Soul claim on forum non conveniens or any other grounds that would route the claim to a non-Colorado forum. Federal courts applying Colorado law to Digital Soul claims shall apply Colorado's non-arbitrability finding as a state public policy determination.

SECTION 10-10-310. INTERSTATE DATA TRANSFER RESTRICTION — JURISDICTION FOLLOWS THE DATA — OFFSHORE PROCESSING PROHIBITION — DATA TRANSFER CERTIFICATION — SUBSIDIARY ROUTING PROHIBITION

10-10-310. Colorado Digital Soul subject to this act regardless of processing location — covered operator registration is jurisdictional hook — offshore processing without CCPAME Data Transfer Certification prohibited — subsidiary routing to avoid jurisdiction prohibited — foreign government data access restriction — reciprocity framework integration.

(1) Jurisdiction follows the data. Colorado resident Digital Soul is subject to this act and Colorado law regardless of: (a) where the data is stored; (b) where the data is processed; (c) the nationality of the entity processing the data; (d) the corporate structure of the covered operator; or (e) any contractual provision purporting to designate non-Colorado law as governing. The covered operator's Colorado registration — and the Colorado resident's Master Deed registration — are the jurisdictional hooks that travel with the data to any location.

(2) CCPAME Data Transfer Certification — required for offshore processing. A covered operator that processes Colorado resident Digital Soul outside the United States or in any state that the CCPAME has not designated as a reciprocating state under §24-20-167 must obtain a CCPAME Data Transfer Certification: (a) certifying that the offshore or non-reciprocating jurisdiction provides protections at least equivalent to Colorado's for the specific data categories being transferred; (b) contractually binding the offshore processor to Colorado's Digital Soul standards as a condition of data access; (c) establishing that the offshore processor is subject to audit by the CCPAME; and (d) ensuring that Colorado residents retain all Digital Soul rights regardless of the processing location. Processing Colorado resident Digital Soul offshore without a valid CCPAME Data Transfer Certification is a Critical Severity Violation.

(3) Subsidiary routing prohibition. A covered operator may not route Colorado resident Digital Soul through a subsidiary, affiliate, joint venture, or contractual partner for the purpose of avoiding this act's requirements. Any processing of Colorado resident Digital Soul by any entity under the covered operator's control, direction, or contractual relationship is attributable to the covered operator for purposes of this act — regardless of corporate structure.

(4) Foreign government data access restriction. Colorado resident Digital Soul held by any covered operator — regardless of processing location — may not be accessed by any foreign government, foreign intelligence service, or foreign law enforcement agency without a judicial warrant issued by a Colorado court of competent jurisdiction. A legal demand from a foreign government under any foreign law — including a UK Investigatory Powers Act order, a Chinese Cybersecurity Law data demand, or any other foreign legal mechanism — does not authorize access to Colorado resident Digital Soul. The covered operator shall notify the ODO within twenty-four (24) hours of receiving any foreign government data demand.

SECTION 10-10-311. CRIMINAL PENALTIES — FELONY DIGITAL SOUL VIOLATIONS — CLASS 4 AND CLASS 5 FELONIES — INDIVIDUAL OFFICER AND DIRECTOR LIABILITY — COLORADO CRIMINAL CODE AMENDMENTS

10-10-311. Criminal penalties for intentional Digital Soul violations — under-13 commercial processing Class 4 felony — DNA bankruptcy sale Class 4 felony — Operator Loyalty betrayal Class 5 felony — Physical Isolation Mechanism circumvention Class 5 felony — individual corporate officer liability — Colorado Criminal Code amendment — mens rea requirement — safe harbor for good faith compliance.

(1) Legislative finding. The general assembly finds that civil penalties alone are insufficient deterrence for intentional, high-value Digital Soul violations — when the commercial gain from violation exceeds the expected civil penalty discounted by enforcement probability, rational actors choose to violate. Criminal penalties change the calculus at the board level — corporate officers and directors face personal criminal liability that cannot be indemnified by the corporation, cannot be discharged in bankruptcy, and cannot be transferred to a successor entity.

(2) Class 4 felony violations. The following are Class 4 felonies under C.R.S. §18-1.3-401: (a) Intentional commercial processing of the Digital Soul of a Colorado resident known or reasonably knowable to be under the age of thirteen (13) — each affected minor is a separate count; (b) Intentional sale, transfer, or licensing of Colorado resident DNA or genetic data in any bankruptcy proceeding, asset sale, or corporate transaction, in violation of §15-15-171(5) — each affected resident is a separate count; (c) Intentional transfer of Colorado resident reproductive health data to any law enforcement agency without a Colorado court warrant, in violation of §15-15-180(3)(a) — each affected resident is a separate count; and (d) Intentional operation of a covered automation system against its registered owner's interests in material breach of the Operator Loyalty Obligation under §10-10-303(6) — where the breach causes actual financial harm exceeding ten thousand dollars ($10,000) to the owner.

(3) Class 5 felony violations. The following are Class 5 felonies under C.R.S. §18-1.3-401: (a) Intentional circumvention, disabling, or bypass of a CCPAME-certified Physical Isolation Mechanism under §10-10-308(3) — each device is a separate count; (b) Intentional deployment of a covered automation system to conduct AI-assisted voter targeting using

Colorado Voter Digital Soul in violation of §15-15-170(6) — each targeted voter is a separate count; (c) Intentional operation of a covered automation system using an encryption backdoor in violation of §10-10-303(7); and (d) Intentional filing of a false Annual AI Ethics Disclosure under §10-10-307 that materially misrepresents the covered operator's training data, objective function, or bias audit results.

(4) Individual corporate officer and director liability. For criminal violations under subsections (2) and (3) committed by a covered operator entity: (a) any corporate officer, director, or managing member who directed, authorized, or knowingly permitted the violation is individually criminally liable — corporate form does not shield individual actors; (b) the prosecution need not prove the individual personally executed the violating act — directing, authorizing, or ratifying the act after discovery is sufficient; and (c) corporate indemnification agreements, D&O insurance policies, and employment agreements purporting to indemnify individuals for criminal liability under this act are void as against public policy to the extent they purport to cover criminal fines and restitution.

(5) Good faith compliance safe harbor. A covered operator or individual who: (a) promptly self-reports a violation to the CCPAME before investigation commences; (b) cooperates fully with the ODO investigation; (c) remediates the violation within sixty (60) days; and (d) pays all applicable civil penalties — is entitled to a prosecution declination for the first self-reported violation. The safe harbor is not available for violations involving minor victims, DNA sale, or reproductive health data transfer to law enforcement.

SECTION 10-10-312. ANTI-SLAPP EXPRESS INCORPORATION — STRATEGIC LAWSUIT PROHIBITION — $50,000 MANDATORY DAMAGES — PRIVATE ATTORNEY GENERAL PROVISION — BOUNTY STRUCTURE

10-10-312. Anti-SLAPP express incorporation — covered operator suits against resident Digital Soul rights exercises are SLAPPs — mandatory dismissal with attorney fees and $50,000 damages — private attorney general provision — 15%/25% bounty on multi-resident enforcement recoveries — qui tam mechanism.

(1) Anti-SLAPP express incorporation. Any legal action — civil, administrative, or otherwise — filed by a covered operator or its affiliate against a Colorado resident arising from the resident's exercise of any right under this act is a strategic lawsuit against public participation (SLAPP) subject to C.R.S. §13-20-1101 et seq. (Colorado's anti-SLAPP statute), as supplemented by this section. Protected activities include: filing a CCPAME complaint; using Live Legal Mode; organizing or joining a Resident Data Cooperative or Farmer Data Cooperative; filing a whistleblower report; submitting a Correction Request; exercising the Universal Telemetry Allowance; activating a Police Encounter Protocol session; and making any public statement about a covered operator's Digital Soul practices. An anti-SLAPP motion shall be filed within sixty (60) days of service of the covered operator's action and shall be heard within thirty (30) days of filing.

(2) Mandatory damages upon SLAPP dismissal. Upon dismissal of a covered operator's action as a SLAPP under this section: (a) the covered operator shall pay the resident's reasonable attorney fees and costs; (b) the covered operator shall pay mandatory statutory damages of fifty thousand dollars ($50,000) per action — not per count, per action; (c) the individual attorneys who filed and prosecuted the SLAPP action are subject to mandatory referral to the Colorado Supreme Court Office of Attorney Regulation Counsel for disciplinary review; and (d) the CCPAME shall note the SLAPP action on the covered operator's Public Accountability Dashboard profile permanently.

(3) Private attorney general provision. A Colorado resident who identifies and brings to successful enforcement a Digital Soul violation affecting multiple residents is entitled to a private attorney general bounty: (a) fifteen percent (15%) of total damages collected where the violation affected one hundred (100) or more residents; (b) twenty-five percent (25%) of total damages collected where the violation affected one thousand (1,000) or more residents. The bounty is paid from enforcement recoveries before remainder flows to affected residents' Resident Automated Mitigation Accounts. Private attorney general actions shall be filed in Colorado courts. Covered operators may not contractually prohibit residents from serving as private attorneys general.

SECTION 10-10-313. PUBLIC HEALTH DATA PROTECTION — EMERGENCY DATA NON-COMMERCIALIZATION — TRIBAL DATA SOVEREIGNTY CONSULTATION — GOVERNMENT-TO-GOVERNMENT PROCESS

10-10-313. Public health emergency data protection — data collected under emergency authorization non-commercial — 90-day post-emergency deletion — AI model training prohibition — tribal data sovereignty — CCPAME government-to-government consultation — tribal Digital Soul framework authority.

(1) Public health emergency data protection. Digital Soul data collected from Colorado residents under any public health emergency authorization — including contact tracing, vaccination records, symptom reporting, quarantine monitoring, and epidemic surveillance — is subject to the following absolute restrictions regardless of any emergency order: (a) may not be used for any commercial purpose including advertising, product development, insurance underwriting, or AI model training; (b) may not be transferred to any non-public-health entity; (c) shall be deleted within ninety (90) days of the end of the declared public health emergency with cryptographic proof of deletion provided to the CCPAME; and (d) shall never be used to train any AI model for any purpose other than the specific public health function authorized. A covered operator that receives public health emergency data under government contract is bound by these restrictions as a condition of the contract and as a statutory obligation independent of any contract term.

(2) Tribal data sovereignty — government-to-government consultation. The CCPAME shall engage in government-to-government consultation with each federally recognized Native American tribe with members residing in Colorado before: (a) promulgating any rule affecting tribal member Digital Soul data; (b) establishing data transfer certification

requirements affecting tribal government operations; (c) designating any tribal territory as a covered operator jurisdiction; and (d) any enforcement action affecting tribal government data systems. Consultation shall occur not fewer than ninety (90) days before any rule takes effect and shall result in a written consultation summary published on the Public Accountability Dashboard.

(3) Tribal Digital Soul framework authority. A federally recognized Colorado tribe may adopt a tribal Digital Soul framework under its sovereign authority that: (a) provides protections at least as comprehensive as this act for tribal member Digital Soul data; (b) establishes a tribal data sovereignty office with CCPAME-equivalent enforcement authority over tribal member data; and (c) enters into a government-to-government data sharing and enforcement cooperation agreement with the CCPAME. Upon adoption of a compliant tribal framework, the tribe's framework governs tribal member Digital Soul data processed on tribal lands — and the CCPAME recognizes the tribal framework as equivalent for interstate reciprocity purposes under §24-20-167.