

RESOLUTION NO. _____

A RESOLUTION OF THE CITY OF PFLUGERVILLE, TEXAS, ADOPTING STANDARDS FOR SECURE, ACCOUNTABLE, FAIR, AND EXPLAINABLE (SAFE) TECHNOLOGY USE; DIRECTING IMPLEMENTATION; AND PROVIDING AN EFFECTIVE DATE

WHEREAS, the City of Pflugerville, Texas (“City”) uses technology to improve public services, accessibility, infrastructure, staff effectiveness, and public safety; and

WHEREAS, artificial intelligence, automated decision tools, surveillance systems, biometric technologies, and external data-sharing networks can create risks to privacy, civil liberties, cybersecurity, safety, fairness, and public trust when used without clear limits and accountability; and

WHEREAS, public trust is strengthened when residents can understand what higher-risk technologies the City uses, why they are used, and what safeguards govern them; and

WHEREAS, artificial intelligence and automated systems should assist rather than replace accountable human judgment, and City employees must remain responsible for City work, actions, and decisions informed by those systems; and

WHEREAS, the 89th Texas Legislature enacted new requirements governing the use of artificial intelligence by local governments, including requirements under Texas Government Code Chapter 2054, Subchapter S, and the Texas Responsible Artificial Intelligence Governance Act (“TRAIGA”), and the Texas Department of Information Resources has adopted implementing rules under 1 Texas Administrative Code Chapter 219; and

WHEREAS, the City Council desires to establish clear standards for technology use, allow the City Manager to administer routine and lower-risk technology, and focus public transparency and Council oversight on technologies that create greater risk;

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF PFLUGERVILLE, TEXAS:

Section 1. Purpose and Governing Policy

The City shall use technology to improve public services, accessibility, efficiency, infrastructure, staff effectiveness, and public safety while protecting City Data, individual rights, and public trust.

The City shall:

1. protect City Data and confidential information;
2. require accountable human judgment when technology affects important City actions or decisions;
3. provide public transparency regarding High-Risk Systems and other technologies identified for public disclosure as required by this Resolution;
4. strictly limit biometric identification, Networked Surveillance Systems, and External Access to City Data;
5. apply safeguards appropriate to the risk presented by a technology; and
6. require City Council approval for High-Risk Systems as provided by this Resolution.

These standards govern the City’s acquisition, pilot, deployment, use, renewal, extension, Material Change, contracting, and external sharing of Covered Systems, whether operated by the City or by another party on its behalf.

They govern City operations and relationships and do not independently regulate private parties.

Section 2. Definitions

For purposes of this Resolution:

“Covered System” means an artificial-intelligence-enabled, automated, data-collection, monitoring, surveillance, analytics, or decision-support system used by or for the City that materially affects:

City services, enforcement, eligibility, public safety, or a Consequential Decision; or

the collection, analysis, retention, search, or sharing of information about identifiable people, vehicles, property, devices, accounts, or businesses.

“City Data” means data generated, collected, received, processed, inferred, derived, analyzed, retained, or maintained by or for the City in connection with City operations.

“Consequential Decision” means a City action involving enforcement, investigation, eligibility, permits, benefits, fines, penalties, discipline, employment, access to City services or facilities, public-safety response, or other adverse treatment of comparable consequence.

“Material Change” means a change to a Covered System that expands or changes its approved purpose, affected population, capabilities, data, integrations, retention, authorized users, External Access, recipients, or permissible uses. Routine maintenance, cybersecurity updates, bug fixes, and configuration changes that remain within the approved scope are not Material Changes.

“Material Incident” means a technology incident that the City Manager or designee reasonably determines involves:

1. unauthorized access to or disclosure of nonpublic City Data;
2. unauthorized External Access or data sharing;
3. use of a system for a prohibited purpose;
4. prohibited facial-recognition or biometric use;
5. failure of required human review in connection with a Consequential Decision;
6. operation of a High-Risk System outside its approved purpose or scope;
7. misuse of a High-Risk System or nonpublic City Data by a City employee or outside party;
8. a cybersecurity incident requiring notification under applicable law or City policy; or
9. comparable harm involving protected rights, physical safety, or loss of City control over nonpublic City Data.

“High-Risk System” means a Covered System that:

1. materially supports or affects a Consequential Decision;
2. is used for law enforcement, investigation, emergency response, public-safety operations, public-space monitoring, Networked Surveillance, biometric identification, or standing or direct External Access;
3. processes sensitive or regulated data outside approved City controls; or
4. presents comparable material risk because of its effects on privacy, civil liberties, physical safety, protected classes, or City control of data.

“Networked Surveillance System” means connected technology or a data-sharing arrangement used, or reasonably capable of being used, to observe, collect, search, analyze, correlate, retain, receive alerts from, or share information about identifiable people, vehicles, devices, activities, or locations.

“External Access” means the ability of a person or entity outside the City to search, query, retrieve, receive alerts from, or otherwise directly access City Data through a City-controlled system.

External Access does not include:

1. the City's authorized ability to search or receive information from another entity's system when that entity receives no access to City Data; or
2. access by a vendor, contractor, or consultant solely as necessary to provide services to the City under a City contract that limits use of City Data to the City's authorized purpose and complies with Section 5.

An outside party's use of City Data for its own purposes or for another customer or entity is External Access and is not covered by the service-provider exception.

Classification under this Resolution depends on the actual or reasonably foreseeable purpose, capability, data, users, access, and use of a system, not its product name, purchasing method, contract structure, vendor description, or technical configuration.

Section 3. Risk Classification and Approval

The City Manager shall classify Covered Systems according to their actual use and risk.

A. Low Risk

A Covered System is Low Risk when it is used for routine productivity, administrative, cybersecurity, infrastructure, or operational purposes, does not process nonpublic City Data about identifiable individuals, and does not meet the criteria for Moderate or High Risk. Low-Risk Systems remain within the City Manager's normal administrative, procurement, information-technology, and departmental authority and do not require individual public listing or separate Council approval under this Resolution.

B. Moderate Risk

A Covered System is Moderate Risk when it processes nonpublic City Data about identifiable people or assists internal City routing, prioritization, forecasting, case management, or staff decisions, but does not support or affect a Consequential Decision and does not meet the definition of a High-Risk System.

The City Manager may approve a Moderate-Risk System after legal, privacy, security, operational, and contractual review appropriate to the system and its use. Moderate-Risk Systems do not require separate Council approval unless otherwise required by law, contract authority, or City policy.

C. High Risk

Before the City first acquires, pilots, deploys, renews, extends, or makes a Material Change to a High-Risk System:

1. City staff shall complete a written review addressing the applicable legal, privacy, security, operational, accessibility, and fairness risks and safeguards;
2. the City shall publish a plain-language public summary; and
3. the City Council must affirmatively approve the system in public.

Council approval shall identify the approved purpose, responsible department, affected people or services, principal risks and safeguards, general categories of data, retention, human-review requirements, External Access, and approval term.

Routine maintenance, cybersecurity updates, and operational changes within the approved scope do not require additional Council approval.

A department may not divide, relabel, stage, restructure, or route a purchase, pilot, contract, capability, or use to avoid a safeguard or Council approval requirement.

The City Manager shall maintain a SAFE Technology Classification Guide providing examples, classification criteria, review requirements, and implementation guidance consistent with this Resolution. The Guide may clarify or provide examples of how this Resolution applies but may not change its definitions, risk classifications, safeguards, or Council-approval requirements.

Section 4. Human Accountability

Artificial intelligence and automated systems may assist City work but may not replace accountable City judgment.

City employees remain responsible for work performed or decisions made with the assistance of those systems.

AI-generated or automated content, summaries, recommendations, alerts, classifications, or analyses may not by themselves serve as the final basis for a Consequential Decision.

Before a Consequential Decision relies on the output of a Covered System, a trained City employee must:

1. understand the system's role and relevant limitations;
2. consider appropriate information outside the system;
3. exercise independent judgment; and
4. have authority to reject, correct, suspend, or override the system's output.

The City Manager shall maintain processes appropriate to system risk for evaluating accuracy, security, continued operational benefit, known limitations, fairness, identified harms, and compliance with approved uses.

Employees shall have a process to report and correct inaccurate, harmful, unauthorized, or noncompliant system outcomes.

No AI System may be used in a manner that unlawfully discriminates against a protected class or otherwise violates legally protected rights or liberties. "AI System" means an artificial intelligence system as defined by Texas Government Code Section 2054.003, as amended.

Section 5. City Data and Contract Protections

The City shall retain all rights it lawfully holds in City Data. A vendor, contractor, consultant, or other outside party may use City Data only for an authorized and lawful City purpose.

Unless expressly approved by the City Council and permitted by law, City Data, including derived or de-identified data, may not be sold, commercialized, used to train a general-purpose model, used to develop an unrelated product or service, used for unrelated profiling, retained beyond the authorized need, or otherwise reused for an independent outside purpose.

Contracts involving a Covered System or outside access to City Data shall include protections appropriate to the system and its risk, including limits on use and access, security and confidentiality, retention and deletion, auditability, incident response, subcontractors, records obligations, and prohibited secondary uses.

The City Attorney may approve alternative contract language providing materially equivalent protections. If a vendor for a Moderate-Risk or High-Risk System will not provide the required protections or a materially equivalent alternative, the City Manager may reject the procurement or bring the exception to Council with the operational need, identified risk, and proposed safeguards.

Existing contracts shall be brought into conformity at renewal, extension, Material Change, or the earliest lawful opportunity.

Section 6. External Access and Data Sharing

The City shall control who may receive or directly access City Data, for what purpose, and for how long. Access and sharing shall be limited to what is reasonably necessary for an authorized and lawful City or governmental purpose.

When a lawful request for specific information can reasonably meet the need, request-based disclosure is preferred over standing, recurring, automated, or direct External Access. When the City can obtain needed information from another entity without giving that entity reciprocal access to City Data, the City should prefer that one-way arrangement when reasonably practicable.

A vendor, contractor, or consultant may access City Data as necessary to perform an authorized service for the City under a contract complying with Section 5. Such access does not authorize the service provider to share City Data with another customer, governmental entity, organization, or third party.

A. Request-Based Sharing

A lawful one-time disclosure does not require separate Council approval when otherwise permitted by law and City policy. The City shall maintain a record sufficient to identify the recipient, purpose, basis, and information disclosed.

A series of individual requests may not be used to create the practical equivalent of standing, recurring, automated, or direct External Access.

B. Standing or Direct Access

Standing, recurring, automated, or direct External Access by another entity requires a written MOU or data-sharing agreement with that entity and City Council approval.

The agreement shall establish the authorized recipients, purpose, data, access, safeguards, retention, auditability, misuse procedures, suspension, and revocation.

Council may approve a framework covering multiple entities when the authorized recipients or categories of recipients, purposes, data, safeguards, and access limitations are defined.

A common vendor, platform, network, purchasing agreement, or contract vehicle does not constitute the required agreement between the City and the entity receiving External Access.

Any addition of a recipient outside the approved scope, expansion of purpose or data, new access capability or network connection, or weakening of an approved safeguard requires additional Council approval.

C. Governmental and Regional Sharing

The requirements above apply to all governmental External Access. Any standing, recurring, automated, or direct External Access by a governmental entity requires Council approval.

Within those requirements, the City should ordinarily prioritize governmental entities that directly serve Pflugerville and governmental partners with general territorial jurisdiction within the Capital Area Council of Governments region.

Standing or direct access for a governmental entity outside that region, or an entity whose jurisdiction is primarily tied to a particular institution, facility, property, transportation system, utility, or other limited-purpose operation, must also have a documented connection to a Pflugerville governmental, investigative, emergency-response, or public-safety need.

For law-enforcement or public-safety access, that connection may include a specific investigation, incident, person, vehicle, location, offense, warrant, missing or endangered person, threat, mutual-aid or officer-safety event, judicial process, or documented multijurisdictional criminal pattern reasonably connected to Pflugerville.

Participation in a regional organization or shared network, general claims of regional crime, or general governmental authority are not sufficient by themselves.

D. Temporary Direct Access

When request-based disclosure would not reasonably meet an active investigative, emergency-response, missing-person, imminent-threat, mutual-aid, or officer-safety need connected to Pflugerville, the City Manager or designee may authorize temporary direct External Access without prior Council approval.

The access must be limited to the necessary recipient, users, purpose, data, capabilities, and duration; documented; auditable; revocable; subject to appropriate use and security restrictions; and expire no later than thirty days after activation.

Temporary access may not be renewed or used successively to create standing access without Council approval.

Temporary access shall be included in the annual SAFE Technology Governance Report at an appropriate aggregate level, subject to applicable investigative, security, privacy, and legal limitations.

Nothing in this Section prevents disclosures required by law, judicial process, established criminal-justice systems of record, emergency response, or lawful case-specific cooperation that does not establish standing or direct External Access.

Section 7. Facial Recognition, Biometrics, and Prohibited Uses

Unless separately authorized by public Council action following City Attorney review and an opportunity for public comment, the City shall not use or benefit from:

1. facial recognition, face comparison, or other biometric technology to identify, verify, search for, track, or profile a person;
2. scraping images, video, audio, internet content, or social-media content for biometric identification;
3. real-time identification of people in a crowd;
4. generalized or suspicionless tracking of lawful First Amendment activity; or
5. social scoring.

Any Council authorization must identify the approved purpose, authorized users, permitted data and capabilities, safeguards, and approval term, and may not permit generalized surveillance or unrelated reuse.

This Section does not prohibit legally authorized criminal-justice identification or evidence functions within an established secured system of record, or non-identifying analytics such as redaction, enhancement, object or event detection, counting, and estimation that do not identify, verify, track, or create identity records for specific people.

Nothing in this Resolution authorizes a use prohibited by state or federal law.

Section 8. Public Transparency and Individual Requests

The City Manager shall maintain a public technology-governance webpage identifying, to the extent legally available:

1. High-Risk Systems;
2. Networked Surveillance Systems;
3. biometric, facial-recognition, identity-search, or comparable identity-based capabilities;
4. standing, recurring, automated, or direct External Access arrangements involving City Data; and
5. other Covered Systems with comparable public impact.

Each entry shall provide a useful public description of the system, responsible department, purpose, vendor when applicable, general categories of data, principal safeguards, and relevant Council approval.

Information may be withheld when disclosure would reveal protected information, create a security risk, or compromise an investigation, or is otherwise protected from disclosure by applicable law.

The City Manager shall maintain an accessible process, which may use existing City intake, contact, or records-request systems, through which a person may:

1. report concerns about a Covered System;
2. request appropriate human review of an automated or AI-assisted City action affecting that person; and
3. request correction of inaccurate factual information.

Section 9. Material Incidents and Annual Reporting

The City Manager shall maintain procedures to identify, contain, investigate, document, and correct potential technology incidents.

A potential incident does not require Council notification solely because it has been reported, alleged, or is under investigation.

The City Manager shall notify Council as soon as practicable, but no later than forty-eight hours after the City Manager or designee reasonably determines that an incident is a Material Incident.

The initial notice may be preliminary and may omit information when disclosure could compromise security, personal privacy, an active investigation, officer safety, privileged legal advice, confidentiality, or other legal obligations.

A written status update shall be provided within ten business days, followed by additional updates and final disposition as appropriate, subject to the same lawful limitations.

No later than ninety days after the end of each fiscal year, the City Manager shall publish and present a consolidated SAFE Technology Governance Report addressing:

1. High-Risk Systems and Material Changes;
2. compliance reviews, Material Incidents, and corrective actions;
3. External Access arrangements and temporary direct-access authorizations;
4. relevant Council approvals and renewals; and
5. reasonably available and reliable measures of the results produced by High-Risk public-safety technologies.

For public-safety and investigative systems, reporting shall distinguish system activity, such as searches or alerts, from verified outcomes, such as investigative leads, cases assisted or solved, arrests, recoveries, or other documented results.

Reporting remains subject to applicable security, privacy, confidentiality, records, and active-investigation limitations.

Section 10. Texas Law and State AI Requirements

The City shall comply with applicable federal and state law governing artificial intelligence and technology, including the Texas Responsible Artificial Intelligence Governance Act (“TRAIGA”), Texas Government Code Chapter 2054, applicable Texas Department of Information Resources rules and standards, and successor or amended requirements.

Those requirements establish minimum standards for City technology governance and supplement the safeguards, classifications, transparency requirements, and Council-approval requirements established by this Resolution unless applicable law expressly provides otherwise.

The City Manager shall implement the officials, inventories, risk assessments, acceptable-use requirements, training, public notices, vendor requirements, records, and other administrative measures required by applicable law and may incorporate them into the City’s SAFE Technology governance processes rather than maintain duplicative procedures.

Section 11. Implementation

Within ninety days after adoption, the City Manager shall:

1. establish the intake and risk-classification process required by this Resolution;
2. complete an initial inventory of known High-Risk Systems, Networked Surveillance Systems, biometric or identity-based systems, and standing or direct External Access arrangements identifiable from existing City records; and
3. publish the initial public technology-governance webpage.

The City Manager shall develop and maintain the SAFE Technology Classification Guide, standard contract protections, review processes, reporting procedures, and other administrative tools necessary to implement this Resolution.

The City Manager shall fully implement the remaining requirements of this Resolution within twelve months after adoption, prioritizing systems and arrangements that present the greatest legal, privacy, cybersecurity, operational, or civil-liberties risk.

Existing data-sharing agreements, MOUs, External Access arrangements, and Covered System contracts shall be reviewed and brought into conformity at renewal, extension, Material Change, or the earliest lawful opportunity.

Section 12. Interim Effect

This Resolution takes effect immediately.

Until the review and approval required by this Resolution are complete, the City shall not newly acquire, pilot, deploy, renew, extend, or make a Material Change to:

1. a High-Risk System;
2. a Networked Surveillance System;
3. biometric or identity-based technology;
4. standing or direct External Access to City Data; or
5. a new vendor right to use City Data for a purpose prohibited by Section 5.

Existing systems may continue within their existing approved purpose and contract term.

Routine maintenance, cybersecurity patching, records preservation, legally required disclosure, and emergency action necessary to address an imminent threat may continue.

No administrative procedure, contract structure, pilot designation, purchasing method, system configuration, or division of a project may be used to evade a Council-approval requirement established by this Resolution.

The City Manager shall return to Council when implementation identifies a legal, operational, security, or practical conflict that requires Council policy direction.

Section 13. Applicable Law and Severability

If applicable law conflicts with this Resolution, law controls only to the extent of the conflict and the remaining provisions continue in effect.

Nothing in this Resolution authorizes conduct prohibited by law.

If any provision or application of this Resolution is held invalid, the remaining provisions and their application to other persons or circumstances remain unaffected.

This Resolution establishes internal City policy and does not create a private cause of action, an independent entitlement to City services, or a basis for liability not otherwise provided by law.

Nothing in this Resolution waives governmental or official immunity, privilege, confidentiality protection, or other defense, or creates contractual rights except through a duly executed City contract.

PASSED AND APPROVED this the ____ day of _____, 2026.

Doug Weiss, Mayor

APPROVED AS TO FORM:

PENDING

Michael C. Hayes, City Attorney

ATTEST:

Trista Evans, City Secretary