RESOLUTION NO.

WHEREAS, the use of surveillance technology for security and public safety by the public and private sector is a familiar and longstanding practice; and

WHEREAS, the capabilities, power, and scope of surveillance technology have advanced rapidly while its use has become more varied and ubiquitous; and

WHEREAS, the ability for surveillance technology to monitor, record, and analyze more aspects of human activity, even enabling the creation of detailed profiles of individuals and their lives, has expanded opportunities to monetize such technology and data; and

WHEREAS, the ability to capture more information about more people in more places can be a powerful resource to aid criminal investigations and prevent and deter crime; and

WHEREAS, the changing nature and use of surveillance technology also increases the incentive to exploit private and intimate personal information for criminal purposes or financial or political gain, and enhances the risk of government overreach, such as targeting politically disfavored groups or the legitimate exercise of constitutional and legal rights; and

WHEREAS, responsible use of increasingly diverse and complex surveillance technologies by the government requires accurate information for officials and the people to weigh and appropriately balance the benefits and harms of such technology; and

WHEREAS, a clear, consistent, and transparent process to disclose and explain how surveillance technology will be used and regulated and when it will require City Council approval is necessary to better inform policy decisions and increase public trust; **NOW, THEREFORE,**

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AUSTIN:

This Resolution is entitled the Transparent and Responsible Use of Surveillance Technology (TRUST) Act.

BE IT FURTHER RESOLVED:

Council directs the City Manager to return to Council not later than its April 23, 2026, meeting with an ordinance amending the City Code to regulate the adoption, acquisition, deployment, use, and review of surveillance technology by any City department.

BE IT FURTHER RESOLVED:

The ordinance shall include, at minimum:

1. A definition of "surveillance technology" that includes any electronic device, system using an electronic device, software, or similar technology that is used, designed, or primarily intended to monitor and collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, neural, or similar information specifically associated with, or capable of being associated with, an individual or group.

    a. Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers (ALPRs), fixed or mobile surveillance cameras, cell-site simulators, International Mobile Subscriber Identity (IMSI) trackers, Global Positioning System (GPS) technology, radio-frequency identification (RFID) technology, biometric surveillance technology, facial-recognition technology, and surveillance systems that aggregate or analyze data for the purpose of monitoring persons or locations in public spaces.

b. With the exception of technology expressly included in the definition of surveillance technology in Subsection 1(a), surveillance technology does not include:

i. Prevalent Technology: Smartphones or general consumer electronics, including cell phones with cameras, microphones, or monitoring capabilities commonly included in commercially available cell phones; and digital recording devices, when used with the consent of those recorded;

ii. Standard Physical Security Tools: Basic security systems such as locks, keycard or badge readers, password-access technology, metal detectors, and standard motion sensors without biometrics functionality;

iii. Standard Business Software and Hardware: Standard business software (e.g., word processors) and standard business hardware (e.g., standard computers);

iv. Information-Technology-Protection Tools: Information-technology-protection tools including, but not limited to, firewalls, data backup, and antivirus software;

v. Medical Equipment: Devices used to diagnose, treat, or prevent disease or injury;

vi. City Data Repositories and Publicly Available Databases: City department data repositories, including, but not limited to, case and record management systems, systems for receiving, documenting, and tracking customer service requests or complaints, systems for geolocating and tracking City

equipment and vehicles, systems for searching and retrieving information from City data repositories, City personnel records, records required to be preserved under open records laws, and publicly available databases;

vii. Non-Digital Observation Tools: Non-digital observation tools used for direct observation without recording capabilities, including, but not limited to, binoculars, telescopes, and night vision goggles;

viii. Communication and Financial Transaction Systems: Standard telephone equipment or systems; standard voicemail equipment or systems; and equipment used to process financial transactions (e.g., credit, debit, and ACH payments);

ix. Technologies used solely for forensic investigation and identification verification of lawfully collected evidence in connection with a criminal incident and which do not surveil the public at large. Examples include forensic laboratory and field equipment, criminal justice databases used exclusively for booking, criminal history record management, or post-incident forensic identification (e.g., fingerprint, DNA, ballistics); evidence-management systems; and advanced 3D scanning technologies for static post-incident crime scene documentation;

x. Jail, prison, or interview room security cameras and court-ordered monitoring systems; or

xi. Cameras that are used solely for traffic control and signal

timing that do not record and retain footage.

2. A definition of "sensitive personal information" that includes the following information about an individual:

   a. Social security numbers, driver's license numbers, and other state identifiers;

   b. Financial data such as account numbers, credit card numbers, and associated credentials;

   c. A person's precise geolocation;

   d. Religious beliefs, ethnic origin, and trade union membership;

   e. Contents of emails and text messages (unless the City is the intended recipient);

   f. Genetic data, biometric information, and health records;

   g. Information about a person's sex life, sexual orientation, or gender identity; and

   h. Personal data collected from a known child, as "child" is defined in 16 C.F.R. § 312.2 (*Definitions*).

3. Unless otherwise provided in Subsections (4) or (7) below, a requirement that City departments obtain Council approval before:

   a. Accepting funds for surveillance technology outside of the annual budget process, including private, state, or federal grants, or donations;

   b. Acquiring new surveillance technology;

   c. Using new or existing surveillance technology or the information it

provides for a purpose or in a manner not previously approved by Council or otherwise required by law; or

d. Entering into an agreement with a third-party entity outside of the City to acquire, share, or use surveillance technology or the information it provides.

4. For any surveillance technology that a City department is seeking to acquire or use in a manner not previously approved by Council, or accepting funds or entering into an agreement therefor, the City Manager or their designee(s), in consultation with the Chief Information Security Officer and the City Attorney's Office, shall prepare a Privacy Impact Assessment. The Privacy Impact Assessment shall be submitted to Council at least two weeks prior to the Council meeting with the item proposed for Council approval and be published online and made available to the public at the same time it is provided to Council; except, in cases involving exigent circumstances, the Privacy Impact Assessment may be provided to Council and the public in accordance with the requirements set forth in Subsection 7(a) below. The Privacy Impact Assessment shall analyze risks to civil liberties and privacy rights and make a determination as to whether the technology poses no or minimal risks to civil liberties and privacy rights. The analysis shall include consideration of the following non-exclusive factors, which if present, shall weigh strongly against a determination that a surveillance technology presents no or minimal risk to civil liberties and privacy rights:

a. The technology allows the indiscriminate collection of data without a warrant, probable cause, or reasonable suspicion of criminal activity, or a criminal nexus where the data is capable of being associated with individuals or groups engaged in legal behavior. Examples include

automated license plate readers and drone cameras deployed on public property.

b. The technology routinely transmits sensitive personal information through data networks subject to legal or illegal access by third parties, other than networks that are completely internal to the City.

c. The technology has the ability to store sensitive personal information in a manner allowing for broad or unrestricted sharing of or access to the information with or by third parties outside of the criminal justice system.

d. The technology has the ability to collect sensitive personal information without a warrant, probable cause, or reasonable suspicion of criminal activity or a criminal nexus, or where the technology allows for the creation of data records associated with particular individuals or groups.

e. The technology collects data in such a manner that it is capable of being used by third parties to develop or expand products, services, or technology, including but not limited to the training of artificial intelligence, other than for the exclusive use by and ownership of the City.

f. The technology or the data it collects is capable of being directly controlled or accessed by third parties outside of the criminal justice system.

g. The technology collects data in such a manner that even if anonymized or compiled, the data can be analyzed or reverse engineered to associate it with individuals or groups .

h. The technology collects data in a manner that is disproportionately associated with a particular demographic, protected class, or the exercise of a constitutionally or statutorily protected right .

i. The technology is capable of collecting sensitive personal information of individuals on their own private property .

j. There have been frequent violations of law, policies, or guidelines associated with the use of the technology in other jurisdictions, the private sector, or previously by the City.

5. For any surveillance technology that requires Council approval under Subsection (3) above, the City Manager or their designee(s) shall submit a proposed Surveillance Use Policy for the surveillance technology to Council at least two weeks prior to the Council meeting with the item proposed for Council approval. The proposed Surveillance Use Policy shall be published online and made available to the public at the same time it is provided to Council. The Surveillance Use Policy shall be developed in consultation with the City department seeking approval of the surveillance technology and reviewed by the City Attorney's Office prior to release and contain, at minimum:

a. Purpose: The specific purposes for the surveillance technology;

b. Technology: A description of the surveillance technology and how it works;

c. Authorized Use: Provisions related to authorized and unauthorized use of the technology and data obtained with the technology, including but not limited to:

i. An exclusive list of the authorized uses of the technology and

the data obtained with the technology;

ii. The rules and processes required before using the technology and the data obtained with the technology;

iii. If applicable, the general location, or types of locations, where the technology may be deployed, unless revealing the locations would compromise criminal investigations;

iv. A description of the machine learning and/or artificial intelligence capabilities and features of the technology, whether use of the technology will provide data for any machine learning and/or artificial intelligence tools, and any guidelines or prohibitions relating to machine learning algorithms and/or artificial intelligence;

d. Data Collection: The information and data elements that the technology collects, including metadata;

e. Data Access: The individuals and entities, including any City department, vendor, subcontractor, service provider, or other third party, who can access or use the collected information, and the rules and processes governing access or use, including whether data will be used by or integrated with artificial intelligence or machine learning algorithms;

f. Data Protection: The safeguards that protect information from unauthorized access, including, but not limited to:

i. Encryption;

ii. Access control;

iii. Anonymization of data;

iv. Differential privacy techniques;

v. Prohibitions on attempting, directly or indirectly, to re-identify any individual from anonymized or de-identified data; and

vi. Access oversight mechanisms;

g. Data Retention: The time period for which information collected by the surveillance technology will routinely be retained, the reason why the retention period is necessary to achieve the purposes of the technology, the process by which the information is regularly deleted after that period lapses, and the conditions that must be met to retain information beyond that period;

h. Public Access: If and how collected information can be accessed by members of the public;

i. Third-Party Data Sharing and Disclosure: If and how non-City entities can access, disclose, or use the information, including:

i. Any required justification and legal standards and requirements to access, disclose, or use the information;

ii. Any limitations on non-City entities' ability to disclose data, including to third-party service providers; and

iii. Any obligation(s) imposed on, or agreements required by, the recipient of the information;

j. Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are or will be any

training materials; and

k. Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including, as applicable, a description of:

i. Personnel responsible for oversight;

ii. Internal and external recordkeeping of use or access to the technology or the information collected, including detailed logging of data accessing events;

iii. Technical measures to monitor for misuse;

iv. Any audit requirements, including whether vendors or other relevant third parties will be required to provide City representatives or independent auditors hired by the City the ability to access any records needed to ensure compliance with the Surveillance Use Policy;

v. Any independent person or entity, inside or outside of the City, with oversight authority; and

vi. Sanctions for violations of the policy.

6. A requirement that all relevant provisions of an approved Surveillance Use Policy shall be incorporated into any contract for surveillance technology between the City and a non-City entity. A copy of the proposed contract for the surveillance technology shall be submitted to Council at least two weeks prior to the Council meeting seeking Council approval of the contract, subject to any legal requirements regarding confidentiality.

7. A process to allow certain exceptions to the requirement to provide a Surveillance Use Policy approved by Council pursuant to Subsections (3)

and (5) above when one of the following applies:

a. Exigent circumstances exist that require a City department to temporarily acquire or use the surveillance technology or the information it provides without obtaining a Surveillance Use Policy approved by Council, provided that:

i. The City Manager or designee(s) finds that such exigent circumstance exist and authorizes the temporary acquisition or use of the surveillance technology in writing. Such authorization shall be disclosed in the report to Council described in 7(a)(iv);

ii. The City Department ceases use of the surveillance technology when the exigent circumstances end;

iii. The City department keeps and maintains only data related to the exigent circumstances, which shall not be shared with or disclosed to any other person or entity unless and only to the extent required for an ongoing investigation, and dispose of any data that is no longer necessary for an investigation, legal process, or audit;

iv. Within 120 days of the use or acquisition of the surveillance technology, the City Manager or their designee(s) must report the acquisition or use of the technology to the Council and explain the exigent circumstances that justified the temporary use or acquisition without Council approval, a general description of the data collected, and if applicable, identification of any third-parties with whom the

data was shared or disclosed;

v. Continued use of the surveillance technology after the exigent circumstances end must be approved by Council through the regular process described in Subsections (3) through (6) above;

vi. The City Manager or designee(s) may extend the period to report, submit a Surveillance Use Policy, and seek Council approval if they certify in writing that disclosing the acquisition or use of the surveillance technology within 120 days would compromise the safety or integrity of an active criminal investigation and specify the duration of the extension. Such certification shall be disclosed in the report to Council following the conclusion of the exigency period, including any extensions. The extension shall be no longer than required to ensure the safety and integrity of an active criminal investigation; under no circumstances shall extensions be provided indefinitely. Extensions shall not be granted for existing exigent circumstances for an unrelated purpose or investigation, which shall be treated as a separate, independent use of surveillance technology; and

vii. Exigent circumstances must be for specific investigative or public safety purposes and not mere convenience. Standard City public safety policies or goals, including but not limited to general crime reduction, traffic safety, or routine law enforcement activities, alone shall not qualify as exigent circumstances.

b. The Privacy Impact Assessment required by Subsection (4) has determined that the surveillance technology at issue presents no or minimal risk to civil liberties and privacy rights such that Council approval is not required.

8. A provision that the following surveillance technologies or data uses are not permitted:

a. facial recognition technology inconsistent with City policy;

b artificial intelligence or machine learning tools inconsistent with City policy; and

c. collection of data for marketing purposes, product development purposes, or any other use that is not necessary to fulfill the terms of a contract but is instead related to the vendor's or other third party's own interests.

9. The City Manager or designee(s) shall submit and present an Annual Surveillance Report to Council at a public meeting within 120 days of the end of each fiscal year. This report shall list each Surveillance Use Policy for surveillance technology the Council approved in the prior fiscal year. For each surveillance technology approved in the prior fiscal year, the Annual Surveillance Report shall describe the surveillance technology and its intended use(s), and shall include, at minimum, the following information for the prior fiscal year:

a. A summary of material non-compliance issues, including but not limited to violations of Surveillance Use Policies that impact(ed) privacy, civil liberties, or civil rights, and any action taken to address the issues;

b. A summary of whether and, if so, how often data acquired through the use of the surveillance technology was shared with outside entities (other than routine sharing through the criminal justice system), the name of any recipient entity or entities, how often the data was shared, the type(s) of data disclosed, and the justification for the disclosure;

c. A summary of whether and how the surveillance technology was used, including whether it captured information regarding members of the public who were not suspected of engaging in unlawful conduct;

d. The results of any non-privileged internal audits, City department self-assessments, or assessments conducted by the City Manager or designee(s);

e. Total annual costs for the surveillance technology, including personnel and ongoing support and maintenance; and

f. An assessment of whether the surveillance technology has been effective at achieving its identified purpose and any obstacles identified to achieving that purpose.

10. Enforcement mechanisms, such as a process for submitting and investigating allegations of violations of Surveillance Use Policies and for achieving City compliance, disciplinary measures for violation of use policies by City employees, and contractual provisions prescribing consequences for violations by non-City entities. Such mechanisms must comply with applicable laws, including the Municipal Civil Service rules.

11. Protections for City employees who make a good-faith complaint to the City Manager, the Austin City Attorney's Office, or a Council member that there has been a violation of surveillance use policies or City Code, as well as

disciplinary actions for City employees for any retaliation against such complainants.

12. A severability provision for any Code provision or Surveillance Use Policy held to be in conflict with state or federal law.

BE IT FURTHER RESOLVED:

For existing surveillance technology acquired, adopted, deployed, or in use by any City department prior to the effective date of the ordinance effectuating this Resolution, the City Manager or designee(s) shall determine, after consultation with the Chief Information Security Officer and the Austin City Attorney's Office, whether the surveillance technology implicates civil liberties or privacy rights based on the criteria in Section 4. If such existing surveillance technology is determined to implicate civil liberties or privacy rights, those City departments must develop a Surveillance Use Policy and obtain the approval of the City Manager or designee(s) of the Surveillance Use Policy within 270 days of the effective date of the ordinance. Except in exigent circumstances, if a City department does not obtain City Manager or designee(s) approval of a Surveillance Use Policy within those 270 days, the department must suspend the use of such existing surveillance technology until the Surveillance Use Policy is approved. The City Manager or designee(s) shall not approve any proposed use policy not in compliance with applicable City Code and policies, including provisions related to this Resolution and other technology policies, including those concerning artificial intelligence and data security. Any approved Surveillance Use Policy under this paragraph shall be made publicly available and included in the next Annual Surveillance Report.

BE IT FURTHER RESOLVED:

The City Manager may designate one or more employees to be responsible for the implementation, oversight, and enforcement of City Code and policies related to surveillance technology or the information it provides, provided that at least one such designee's primary responsibilities shall include (1) oversight, policy development, and/or decision-making authority concerning technology and data privacy and security, and (2) legal matters related to civil rights and civil liberties. Examples include the Chief Privacy Officer, the Chief Information Security Officer, and the City Attorney.

ADOPTED: _____, 2026 **ATTEST:** _____
Erika Brady
City Clerk