Attachment 2: Privacy and Data Principles for the Automated Enforcement Transportation Innovation Challenge (TIC)

This attachment outlines the approach that staff will follow to manage and protect the personal information collected through the TIC. A Privacy Impact Assessment has been initiated with Corporate Information Management Services (CIMS, City Clerk's Office) and will be completed once the roster of TIC participants has been established and their technology solutions have been reviewed.

In addition, an Information Management (IM) Assessment has been completed with CIMS. This Assessment established requirements to manage, store, and safeguard City information collected through the TIC, ensuring compliance with the Toronto Municipal Code, Chapter 217 (Records). The IM Assessment granted a conditional approval to proceed with the TIC, with information management activities and recommendations aligned to the proposed phases of the TIC.

The following principles have been established based on the privacy and information management work that has been undertaken to date and will be used to determine how any personal information collected by the TIC is managed and protected.

1. **Implementing the Digital Infrastructure Strategic Framework (DISF):** The TIC program was developed to explore new technologies in accordance with the Digital Infrastructure Plan (since renamed the Digital Infrastructure Strategic Framework or DISF), which was approved by Council in April 2022. All aspects of the TIC are being developed and delivered in accordance with the DISF, including the following principles.
2. **Embodying privacy-by-design:** Technology developers participating in the TIC will be encouraged to process data (i.e. images and video footage) at the "edge" (i.e. a computer processor is physically connected to each camera). Whereas central processing would involve transmitting continuous raw video footage to a central or cloud-based server, edge processing allows for storage or transmittal of only images or short video segments where a suspected traffic violation has occurred. The majority of the data that is captured by the camera is therefore never stored or transmitted. Edge computing can also enable at-source automatic facial blurring which further reduces the collection of extraneous personal information. A key goal of the TIC is confirm the feasibility of requiring edge computing and / or automatic facial blurring for any future procurement related to automated enforcement.
3. **Establishing data governance in compliance with relevant federal and provincial legislation and applicable City policies:** Data governance for the TIC is being established to comply with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) as well as various City policies, frameworks (such as the DISF) and standard operating procedures. Aspects of the data governance approach for the TIC include:
    - The City will own all data that is collected through the TIC.
    - Data residency in Canada is the expectation for all TIC participants. Exceptions to this would only be made after review and approval by the Office of the Chief Information Security Officer and Corporate Information Management Services.

- Access to the data will be restricted as per section 32 of MFIPPA:

  32 *An institution shall not disclose personal information in its custody or under its control except,*

  (a) in accordance with Part I;

  (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;

  (c) for the purpose for which it was obtained or compiled or for a consistent purpose;

  (d) if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions;

- Data retention will be determined based on the appropriate City record classification in consultation with Corporate Information Management Services, ensuring compliance with Municipal Code Chapter 217.
- The ability to access, manage and analyze data in non-proprietary, machine-readable formats (e.g. csv format) will be prioritized throughout the TIC.
- If an academic institution is engaged to undertake data analysis, an appropriate data sharing agreement would be developed with the academic partner.

4. **Protecting data:** A Cloud Security Assessment will be undertaken for each TIC participant under the guidance of staff in the Office of the Chief Information Security Officer (CISO) in order to assess the cyber security readiness of the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud environments.
5. **Maximizing learning:** The purpose of the TIC is to help the City i) make informed decisions about any future expansion to the City's automated enforcement program; and ii) engage with the Province on this topic in a more fully informed way. To achieve this, the TIC will explore a broad range of issues related to automated enforcement, including data governance, information management, cybersecurity and privacy protection by engaging relevant City-internal subject matter experts. A public report will be released after the TIC is completed to summarize key findings and future implications for automated enforcement in Toronto.