RECORD OF CREATION OF NON-PERSONAL DATA
(Internal Use Only)

Under the *Protection of Privacy Act* (**POPA**), The City of Calgary (**COC**) is required to create and maintain a record each time non-personal data is created. Please refer to the accompanying *NPD Creation and Deidentification Guide* and examples if additional details are needed.

Non-Personal Data (**NPD**) means data, including data derived from personal information and synthetic data, that has been generated, modified or anonymized so that it does not identify any individual directly or indirectly.

NPD must be created in accordance with generally accepted best practices.

DEPARTMENT AND BUSINESS UNIT:	
DIVISION:	
CONTACT PERSON (NAME AND POSITION):	
CONTACT EMAIL ADDRESS:	
DATASET AND/OR SYSTEM NAME (OPTIONAL):	
DATE OF NPD CREATION OR REFRESH:	

---

1. What is this dataset about? What are the keywords you would use to describe this dataset? Use complete sentences and include keywords that might be helpful when searching for this record.

   NOTE: Reference examples of answers provided in the NPD Creation and Deidentification Guide

2. The City of Calgary may only create non-personal data for one or more of the following purposes. What is the purpose for creating the non-personal data? Select all that apply. *(GOA Fact Sheet)*

   ☐ Research and analysis

   ☐ Planning, administering, delivering, managing, monitoring or evaluating a program or service

   NOTE: If your purpose does not fall within one of the options above, or if you are unsure, do not continue. Contact the Privacy Officer at AccessandPrivacy@calgary.ca before proceeding with the creation of NPD.

3. How will these data be shared? Select all that apply.

   ☐ Internal – within the City of Calgary only

   ☐ External – other public bodies

   ☐ External – non-public bodies (e.g. vendors, researchers)

   ☐ Public release (e.g. reports, dashboards, open data portal)

4. What categories of identifiers and associated risk-relevant elements were present in the source data, and required consideration or transformation?

   Part A – Categories of identifiers (select all that apply)

   These options flag categories of possible identifiers that required attention. Select all that apply.

   ☐ Direct identifiers

   ☐ Indirect (quasi-) identifiers

   ☐ Sensitive attributes

   NOTE: All risks are assessed in detail in Question 7 (Risk Matrix)

Part B – Associated privacy risk elements (select all that apply)

These categories describe the kinds of data attributes involved. They group related examples explained in detail in the *Risk Assessment for Re-identification Guide*. Select all that apply. If unsure, select the closest match and explain in "Other."

☐ Identity and contact information
☐ Demographic or personal characteristics
☐ Employment or organizational attributes
☐ Geographic or location-based information
☐ Dates or time-based information
☐ Household or relationship attributes
☐ Sociodemographic or population attributes
☐ Behavioural or transactional data
☐ Small population or uniqueness indicators
☐ Others (describe): _____

5. **What personal information existed before transformation?**

Briefly note the personal information and specific data elements or combinations (e.g., field names, attributes, patterns, or small groups) that were most relevant to re-identification risk in this dataset.

NOTE: For more examples and additional guidance, see the NPD Creation and De-Identification Guide or contact the Privacy Officer at AccessandPrivacy@calgary.ca.

6. Describe the method used to create the non-personal data. Select all that apply.

Methods used (check all applicable):

☐ Pseudonymization
☐ Aggregation
☐ Suppression
☐ Generalization
☐ Noise Injection
☐ Synthetic Data
☐ Other: _____

NOTE: Refer to Section 4 in the Guide: How to De-Identify Data

7. Describe the assessment performed to determine whether the residual risk of identifying or re-identifying individuals is low enough to treat the dataset as non-personal data. Select all that apply.

☐ COC Re-Identification Risk Assessment Matrix **(Final Score: _____)**

Identifiability =	**S**ensitive Attributes =	**L**inkage Risk =	**G**ranularity =	**C**ontext & Controls =

☐ Reviewed and approved by Corporate Privacy team
☐ Other: _____

Recertification, Review, Check-In

Next Recertification Criteria	When dataset structure, linkage context, or release model changes, or every 3 years.
Provisional Next Recertification Date	Date:

Check-In Date with the Privacy Officer	
Business Unit Manager	

Additional resources available:

- Guide to completing the NPD creation form
- Risk Assessment for Re-identification Guide