

DATA SHARING AGREEMENT

Between

Snohomish County 911

and

CITY OF EVERETT (EVERETT POLICE DEPARTMENT)

This Data Sharing Agreement ("**DSA**") is entered into between Snohomish County 911 ("**SNO911**") and CITY OF EVERETT (EVERETT POLICE DEPARTMENT) ("**Agency**"). on this 2ND day of MAY, 2024.

Data Provider: Snohomish County 911

Contact Name: MARLIN HEROLAGA
Title: DIRECTOR OF TECHNOLOGY
Address: 1121 SE Everett Mall Way, Suite 200, Everett, WA 98208
Phone: 425-407-3911
Email: MHEROLAGA@SNO911.ORG

Entity Receiving Data: EVERETT POLICE DEPARTMENT

Contact Name: JOHN DEROUSSE
Title: POLICE CHIEF
Address: 3002 WETMORE AVE, EVERETT, WA 98201
Phone: 425-257-8408
Email: JDEROUSSE@EVERETTWA.GOV

1. BACKGROUND

SNO911 hosts various shared systems accessed by the entire Snohomish County Public Safety agencies. These systems contain all category data especially category 3 and category 4 data that must be protected. The agreement below applies to shared systems, including but not limited to Computer-Aided Dispatch (CAD), Records Management Systems (RMS), Corrections, Patient Care Reporting, data reporting & analytics, and other systems.

2. PURPOSE OF THE DSA

The purpose of the DSA is to provide the requirements and authorization for SNO911 to exchange confidential information with the Agency to ensure compliance with legal requirements pursuant to RCW 39.34.240 and to maintain sharing of data as allowed by and

subject to any limitations in Chapter 42.56 RCW or other applicable state or federal law in the handling of information considered confidential.

3. DEFINITIONS

"Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

"Authorized User" means an individual or individuals with an authorized business need to access Confidential Information under this DSA.

"Confidential Information" means category three or higher data as defined in policy established in accordance with RCW 43.105.054 and information allowed to be kept from public disclosure under RCW 39 chapter 42.56 RCW or as elsewhere provided by state or federal law.

"Data Access" refers to rights granted to the Agency employees to receive confidential SNO911 data or to directly connect to SNO911 systems, networks and/or applications combined with required information needed to implement these rights.

"Data" means the information that is disclosed or exchanged as described by this DSA. For purposes of this DSA, Data means the same as "Confidential Information."

"Data Transmission" refers to the methods and technologies to be used to share data or to move a copy of the data between systems, networks and/or employee workstations.

"Data Storage" refers to the place data is in when at rest. Data can be stored on removable or portable media devices that is provided by the Agency such as a USB drive or SNO911 managed systems.

"Data Encryption" refers to enciphering data with an approved algorithm or cryptographic module. Encryption must be applied in such a manner that it renders data unusable to anyone but the authorized Agency user.

"DSA" means this Data Share Agreement.

"RCW" means the Revised Code of Washington. All references in this DSA to RCW chapters or sections will include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at: <http://apps.leg.wa.gov/rcw/>.

"Receiving Party" means the party who is the recipient of Data.

"Regulation" means any federal, state, or local regulation, rule, or ordinance.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

"Subcontract" means any separate agreement or contract between a Receiving Party and an individual or entity ("Subcontractor") to perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

"Subcontractor" means a person or entity that is not in the employment of the Receiving Party, who is performing services or any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

4. PERIOD OF AGREEMENT*

This DSA shall begin on its effective date and end when **[the Agency ceases to be a SNO911 member agency] OR [the subscribing Agency's agreement with SNO911 terminates]**, unless terminated sooner by the parties' mutual written decision.

5. JUSTIFICATION FOR DATA SHARING

The Agency operates critical public safety services for its jurisdiction. SNO911, as the operator for the Snohomish County 911 service, carefully coordinates its public safety services with the Agency. In the course of providing, monitoring, and assessing its provision of those services, each party needs access to data, including confidential records, during the course of its operations.

6. DATA CLASSIFICATION

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer (OCIO) and included in OCIO Standard No. 141.10.

The Data that is the subject of this DSA is classified as indicated below:

- Category 1 – Public Information
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.
- Category 2 – Sensitive Information
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.
- Category 3 – Confidential Information
Confidential information is information that is specifically protected from release or disclosure by law. It may include but is not limited to:
 - a. Personal Information about individuals, regardless of how that information is obtained
 - b. Information concerning employee personnel records
 - c. Information regarding IT infrastructure and security of computer and telecommunications systems;

- Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

- a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements
- b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions

7. DESCRIPTION OF DATA TO BE SHARED

The data to be shared includes information and data related to operations and compliance with contractual, state, and federal programs, security of computer systems, and performance data.

8. DATA ACCESS

SNO911 may provide the Agency direct, read-only access into select internal systems. SNO911 will provide system access only in support of demonstrated need for the providing, monitoring, and assessment of Agency's public safety services. Agency agrees to notify SNO911 when access is no longer needed.

9. DATA TRANSMISSION

Transmission of data between SNO911 and the Agency will use a secure method that is commensurate to the sensitivity of the data being transmitted.

10. DATA STORAGE AND HANDLING REQUIREMENTS

All confidential data provided by SNO911 will be stored with access limited to the least number of Agency staff needed to complete the purpose of this DSA.

11. CONSTRAINTS ON USE OF DATA

Agency will strictly limit use of information obtained under this DSA to the purpose of carrying out its public safety obligations. Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

12. SECURITY OF DATA

Agency will protect and maintain all Confidential Information gained by reason of this DSA against unauthorized use, access, disclosure, or loss. Agency will comply with industry standard practices and policies for data security and access controls to ensure the confidentiality, and integrity of all data shared. This includes restricting access to the Confidential Information by:

- a. Allowing access only to staff that have an authorized business requirement to view the Confidential Information. Such staff must be properly trained in security awareness.
- b. Physically securing any computers, documents, or other media containing the Confidential Information.

- c. Agency shall promptly report all data breaches or other security incident involving the shared data to SNO911's Data Compliance Officer within (1) business day of the discovery. Such reports shall include all relevant details of the security incident, including the scope, impact, and remediation efforts.

13. DATA INFORMATION DISPOSAL

Under this DSA, the Agency must take on the responsibilities to take all reasonable steps to destroy or arrange for the destruction of data obtained by this DSA in accordance with Washington State Law.

14. NON-DISCLOSURE OF DATA

Agency must ensure that all employees or Subcontractor(s) who will have access to the Data described in this DSA (including both employees who will use the Data and IT support staff) are instructed and made aware of the use restrictions and protection requirements of this DSA before gaining access to the Data identified herein. The Receiving Party will also instruct and make any new employee aware of the use restrictions and protection requirements of this DSA before they gain access to the Data.

15. OVERSIGHT

SNO911 reserves the right, at any time, to monitor, audit, and review activities and methods used to implement this DSA to assure compliance.

16. NON-WAIVER OF OBLIGATIONS

If this DSA is terminated for any reason, once data is accessed by the Agency, this DSA is binding as to the confidentiality, use of the data, and disposition of all data received as a result of access, unless otherwise amended by the mutual agreement of both parties. This provision will survive the termination or expiration of this DSA.

17. RESPONSIBILITY

Each Party to this DSA will be responsible for the negligent acts or omissions of its own employees, officers, or agents in the performance of this DSA. No Party will be considered the agent of another Party and no Party assumes any responsibility to another Party for the consequences of any act or omission of any person, firm, or corporation not a party to this DSA. Agency agrees to comply with all applicable state security and privacy requirements associated with the data being shared.

18. SEVERABILITY

The provisions of this DSA are severable. If any provision of this DSA is held invalid by any court of competent jurisdiction, that invalidity will not affect the other provisions of this DSA and the invalid provision will be considered modified to conform to the existing law.

19. AMENDMENT

This DSA only may be amended by the mutual consent and approval of both parties. No additions or alterations of this DSA's terms will be valid unless made in writing, formally approved, and executed by each party's duly authorized agents.

20. WAIVER

Waiver of any breach or default on any occasion will not be deemed to be a waiver of any subsequent breach or default. Any waiver will not be construed to be a modification of the terms and conditions of this DSA.

21. NO ASSIGNMENT

Neither party may transfer or assign part or all of its responsibilities or rights under this DSA without the other party's prior written consent.

22. SIGNATURES AND COUNTERPARTS

By signing below, the parties acknowledge their acceptance of this DSA, which will take effect on the last date signed below. The Parties may execute this DSA in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement.

Snohomish County 911

Marlin M Herolaga

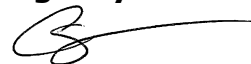
Digitally signed by Marlin M
Herolaga
Date: 2024.05.02 11:22:48 -07'00'

Name: MARLIN HEROLAGA

Title: DIRECTOR OF TECHNOLOGY

Date: May 2, 2024

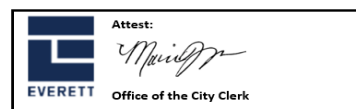
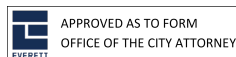
Agency



Name: Cassie Franklin

Title: Mayor

Date: 05/28/2024














EVERETT PD SNO911 DSA _2024-05-23_SD

Final Audit Report

2024-05-28

| | |
|-----------------|---|
| Created: | 2024-05-28 |
| By: | Marista Jorve (mjorve@everettwa.gov) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAyKQJLIhhgsbHZYhOpbQK_KxNG6ZBZWX |

"EVERETT PD SNO911 DSA _2024-05-23_SD" History

-  Document created by Marista Jorve (mjorve@everettwa.gov)
2024-05-28 - 8:20:12 PM GMT
-  Document emailed to Alicia Gill (AGill@everettwa.gov) for approval
2024-05-28 - 8:20:51 PM GMT
-  Email viewed by Alicia Gill (AGill@everettwa.gov)
2024-05-28 - 8:25:03 PM GMT
-  Document approved by Alicia Gill (AGill@everettwa.gov)
Approval Date: 2024-05-28 - 8:25:15 PM GMT - Time Source: server
-  Document emailed to Tim Benedict (TBenedict@everettwa.gov) for approval
2024-05-28 - 8:25:16 PM GMT
-  Email viewed by Tim Benedict (TBenedict@everettwa.gov)
2024-05-28 - 8:25:25 PM GMT
-  Document approved by Tim Benedict (TBenedict@everettwa.gov)
Approval Date: 2024-05-28 - 8:25:41 PM GMT - Time Source: server
-  Document emailed to Cassie Franklin (cfranklin@everettwa.gov) for signature
2024-05-28 - 8:25:43 PM GMT
-  Email viewed by Cassie Franklin (cfranklin@everettwa.gov)
2024-05-28 - 8:26:14 PM GMT
-  Document e-signed by Cassie Franklin (cfranklin@everettwa.gov)
Signature Date: 2024-05-28 - 8:26:22 PM GMT - Time Source: server
-  Document emailed to Marista Jorve (mjorve@everettwa.gov) for approval
2024-05-28 - 8:26:23 PM GMT

 Document approved by Marista Jorve (mjorve@everettwa.gov)

Approval Date: 2024-05-28 - 8:27:50 PM GMT - Time Source: server

 Agreement completed.

2024-05-28 - 8:27:50 PM GMT