DATA EXCHANGE COMPACT
AMONG
PARTICIPATING AGENCIES OF [XX]

This Data Exchange Compact (DEC) is effective on the date the Participating Agencies sign this DEC. Any specific scope or exchange of information or data relating to a subset of Participating Agencies under the terms of this DEC are identified in Attachment 1 to this DEC, "Scope of Information Exchange."

ARTICLE 1. PURPOSE

The purpose of this DEC is to:

(1) Facilitate disclosure of or access to data as defined in the Scope of Information Exchange (Attachment 1) to the Receiving Agency. Additional information around data classifications are defined in the data lexicon (attached).

(2) Describe each Participating Agency's rights and obligations with respect to the confidential information and the limited purposes for which Receiving Agency may use or have access to confidential information.

Data sharing under this agreement will be limited to the purposes described herein, consistent with the applicable legal authorities defined in Articles 2 and 6 and Attachment 1.

ARTICLE 2. AUTHORITY

The Participating Agencies enter into this DEC under the authority of [INSERT APPLICABLE STATE-LEVEL AUTHORITIES] as defined in Attachment 1 as well as the specific authority of each Participating Agency.

ARTICLE 3. DEFINITIONS

These definitions as well as those found in applicable laws and industry frameworks, incorporated as listed in Attachment 1, will apply to this DEC. Other terms will be defined based on their plain meaning or other statutory definitions.

"AI" or "Artificial Intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[1] AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

"AI system": Any system, software, sensor, or process that automatically generates outputs including, but not limited to, predictions, recommendations, or decisions that augment or replace human decision-making. This extends to software, hardware, algorithms, and data generated by these systems, used to automate large-scale processes or analyze large data sets.

"Authorized Purpose" means the specific purpose or purposes described in Attachment 1, Scope of Information Exchange of this DEC for the specific Participating Agencies to fulfill the obligations under the Scope of Information Exchange or any other purpose expressly authorized in writing in advance.

"**Authorized Representative"** means an individual who has the signatory authority to enter into legally binding agreements on behalf of their agency or organization.

[1] Definition from 15 U.S.C. 9401(3).

"Authorized User" means a person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze confidential information pursuant to this DEC;

(2) For whom a specific Participating Agency requesting information represents has a demonstrable need to create, receive, maintain, use, disclose, or have access to the confidential information;

(3) Who has agreed in writing to be bound by a Participating Agency's requirements regarding disclosure and use of confidential information as required by this DEC; and

(4) Who has completed training in privacy, security, and breach response as required by the applicable laws under this agreement and who has agreed to be bound by the terms of this DEC.

Automated Decision-Making Technology (ADMT): ADMT refers to systems or processes that make decisions without human intervention based on pre-defined rules, algorithms, or AI-generated insights. ADMT systems typically focus on achieving specific outcomes efficiently and reliably, often by automating repetitive or structured tasks.

"**Breach**" means an incident that results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses protected information under applicable law listed in this agreement or an authorized user accesses or potentially accesses such information for other than authorized purposes.[2]

"Incident" means an attempted or successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system. An incident can be caused by factors including but not limited to a person, organization, or an Automated Decision Making Technology.

"**Industry standards**" mean as applicable, codes, guidance (from regulatory and advisory bodies, whether mandatory or not), international and national standards, relating to security of network, and security breach and incident reporting requirements, all as amended or updated from time to time, and including but not limited to the current standards and benchmarks listed in Attachment 1, in accordance with the latest revisions and/or amendments.

"[Information] or [Data]" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.[3] This includes metadata.

"Metadata" means data that describes or gives information about other data.

"[Personal Data] or [Personally Identifiable Information (PII)]" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[4]

"Record" means a collection of information or facts registered on paper or electronic media as a means to preserve knowledge.

ARTICLE 4. DUTIES OF A DISCLOSING AGENCY

[2] Adapted from the National Institute Standards of Technology Special Publication 800-53 Rev 5
[3] Definition from NIST SP 800-30 Rev.1
[4] Definition from NIST SP 1800-27B

4.1. Disclosing Agency will transmit the information as specified in the Scope of Information Exchange in a secure manner to Receiving Agency.

4.2. Disclosing Agency will comply with all laws and regulations applicable to the type of information disclosed.

4.3. Disclosing Agency will implement appropriate data validation rules to confirm that the information to be exchanged is accurate and complete as specified in the applicable policies and procedures documents referenced in Attachment 1. Disclosing Agency represents that at the time of transmission, the information it provides is an accurate representation of the data described in the Scope of Information Exchange.

4.4. Disclosing Agency will conduct necessary evaluations of the information to be shared to ensure the confidentiality, integrity, and availability of data meets all privacy and security industry standards.

ARTICLE 5. DUTIES OF A RECEIVING AGENCY

5.1. Receiving Agency will exercise reasonable care to protect confidential information from being used in a manner other than the Authorized Purpose or by other than an Authorized User. Receiving Agency will only disclose confidential information to Authorized Users to the extent necessary to accomplish the Authorized Purpose and as permitted by law. Receiving Agency will establish, implement, and maintain administrative, physical, and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the confidential information.

5.2. Receiving Agency will maintain updated privacy, security, and breach response policies and procedures as required by law or internal policies.

5.3. Receiving Agency will not disclose confidential information to any person other than an Authorized User, or as required by law.

5.4. Receiving Agency will establish, implement, and maintain corrective actions against any member of its workforce or subcontractor who fails to comply with this DEC.

5.5. Receiving Agency will be directly responsible for the compliance of its subcontractors with this DEC and any enforcement of this DEC with respect to its subcontractors.

5.6. Receiving Agency will promptly notify Disclosing Agency of any requests for amendments to confidential information, access to confidential information by the individual subject of the confidential information, or record of disclosures of confidential information.

5.7. Receiving Agency will maintain an accounting of all disclosures of confidential information.

5.8. Upon termination of the Scope of Information Exchange, Receiving Agency will return or destroy confidential information received from Disclosing Agency to the extent reasonably feasible and permitted by law. The return and/or destruction will be documented by the Receiving Agency. If Receiving Agency is required by law or litigation hold to retain confidential information beyond the termination of the Scope of Information Exchange, Receiving Agency will continue to safeguard the confidential information in accordance with this DEC.

5.9. If Receiving Agency transmits or stores confidential information via electronic means, Receiving Agency will utilize secure file transfer protocol or encryption in motion and at rest and other applicable security controls in accordance with the most current version of the National Institute of Standards in Technology, Special Publication 800-53, or other equally protective security controls.

5.10. Receiving Agency will designate a privacy official and a security official, who may be the same individual, authorized to act on behalf of the Receiving Agency with respect to implementing the privacy and security requirements in this DEC. Receiving Agency will provide contact information for these officials to Disclosing Agency.

5.11. Receiving Agency will timely cooperate with any request for information, documentation, audit, inspection, or investigation by any applicable regulatory authority or as required by Disclosing Agency to comply with its regulatory requirements.

5.12. Receiving Agency will comply with all laws and regulations applicable to the type of confidential information including but not limited to Attachment 1 as applicable.

ARTICLE 6. MUTUAL OBLIGATIONS AND RESPONSIBILITIES

6.1. Performance of Obligations; Compliance with State and Federal Law.

All Participating Agencies shall diligently perform all obligations arising hereunder and shall comply with all applicable laws and regulations, as defined in Attachment 1, the Scope of Information Exchange, and the requirements therein to develop capabilities, policies and procedures to protect the information defined therein. The parties will neither use nor disclose shared information in a manner inconsistent with the terms of this agreement.

6.2. System Security & Privacy.

Participating Agencies shall implement privacy and security measures with respect to access to and use of the information and associated systems in compliance with the terms in this agreement and standards listed in Attachment 1.

6.3. Information Security and Cybersecurity Measures.

6.3.1 Participating Agencies shall implement, and at all times maintain, appropriate administrative, technical, and physical measures to protect and secure the information exchanged as part of this agreement, that is accessible to, or held by, another Participating Agency. At a minimum, such measures shall conform with the generally recognized Indusrty Standards and best practices, and shall comply with applicable privacy and data security laws, including implementing and maintaining administrative, technical, and physical safeguards pursuant to applicable U.S. federal, state, and local laws and regulations as defined in Attachment 1.

6.3.1.1 Policies, Procedures & Practices. Receiving Agency must have policies, procedures and practices that address its information security and cybersecurity measures, safeguards, and standards, which Disclosing

Agency shall be permitted to audit via written request, and which shall include at least the following:

a) Passwords and Other Security Mechanisms. Receiving Agency shall issue a username and password and/or other security measure for each identified Authorized User to access Receiving Agency systems that contain information provided by the Disclosing Agency. Receiving Agency shall be responsible for transmitting the username and password to the appropriate Authorized User. When Receiving Agency removes an individual from its list of Authorized Users, it shall promptly cancel and de-activate the username and password of the identified individual.

b) Access Controls. Access controls, including multi-factor authentication, to limit access to the information provided by the Disclosing Agency;

c) Encryption. Use of encryption to protect information in transit and at rest, accessible to or held by Receiving Agency;

d) Security. Safeguarding the security of the information accessible to or held by Receiving Agency, which shall include hardware and software protections such as network firewall provisioning, intrusion, and threat detection controls designed to protect against malicious code and/or activity, regular (two or more annually) third party vulnerability assessments, physical security controls, and personnel training programs that include phishing recognition and proper data management hygiene; and

e) Software Maintenance. Software maintenance, support, updates, upgrades, third party software components and bug fixes such that the software is, and remains, secure from vulnerabilities in accordance with a minimum of one the applicable Industry Standards as defined in this agreement.

6.3.1.2 Technical Standards. Receiving Agency shall comply with the following requirements and technical standards related to network and data security.

a) Network Security. At minimum, network security shall conform with at least one of the applicable and generally recognized Industry Standards as defined in this agreement.

b) Cloud Services Security: If Receiving Agency employs cloud technologies, including infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS), Receiving Agency shall adopt a "zero-trust architecture" satisfying the requirements described in NIST 800-207 (or any successor cybersecurity framework thereof), unless another standard or approach has been approved in advance by Disclosing Agency, whose approval shall not be unreasonably withheld.

c) Data Storage. Receiving Agency agrees that any and all data shared will be stored, processed, and maintained solely on designated target servers or cloud resources. No shared data, at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless approved by Disclosing Agency or unless that device or storage medium is in use as part of Receiving Agency's designated backup and recovery processes and is encrypted in accordance with the requirements set forth herein.

d) Data Encryption. Receiving Agency agrees to store all data shared as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Receiving Agency further agrees that any and all shared data stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed in accordance with at least one of the applicable the Industry Standards defined in this agreement.

e) Data Transmission. Receiving Agency agrees that any and all electronic transmission or exchange of system and application data with any other parties expressly designated by this agreement shall take place via secure means in accordance with at least one of the applicable Industry Standards defined in this agreement.

f) Data Re-Use. Receiving Agency agrees that any and all shared data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement.

ARTICLE 7. NOTICES

7.1. Unless otherwise provided in this agreement, all notices, demands, requests, approvals or other communications which may be or are required to be given, served or sent pursuant to this agreement shall be in writing.

7.2. Notice will be given to the parties specified in the Scope of Information Exchange by [INSERT PREFERRED METHOD OF NOFTIFICATION RECEIPT, E.G. EMAIL].

7.3. Parties will specify the time in which they would like to be notified regarding the exchange and usage of information. This can include but not limited to notices related to:

7.3.1 Receipt or sending of data

7.3.2 Security "incidents" or "breaches" as defined in this agreement that impact the data exchanged

7.3.3 Data subject use and sharing notification, as applicable

7.3.4 Additional notice requirements listed throughout this agreement.

7.3.5 Media coverage

ARTICLE 8. SECURITY INCIDENT AND BREACH RESPONSE, REPORTING, AND CORRECTIVE ACTION

8.1. The Participating Agencies will comply with the Incident and Breach reporting, notification, and corrective action requirements in accordance with applicable laws defined in Attachment 1, the Scope of Information Exchange. Participating Agencies must report a Breach to the applicable oversight agencies listed in Attachment 1.

8.2. For the purposes of the DEC, the definitions as listed in this DEC apply unless otherwise agreed upon by parties within the Scope of Information Exchange.

8.3. Both Receiving Agency and Disclosing Agency agree to comply with all applicable data protection and privacy laws and regulations. Both agree to implement best practices for incident management to identify, contain, respond to, and resolve Incidents.

8.3.1 In the event of an Incident, including a ransom or extortion request that affects information as defined in the Scope of Information Exchange, the Participating Agency that is aware of the incident shall notify all other Participating Agencies' Chief Information Security Officer(s) [OR EQUIVALENT SECURITY MANAGER/OFFICER] by telephone and email as provided in the Scope of Information Exchange, "Contact Information for Notices" as promptly as possible, but in [no event later than twenty-four (24) hours from discovery of the Incident : OR INSERT APPLICABLE STATE INCIDENT RESPONSE TIME NOTIFICATION REQUIREMENTS HERE]

8.3.2 In the event of an Incident or Breach, the agency experiencing the incident will, at the other agencies' request, (i) fully cooperate with any investigation concerning the Incident or Breach by the other Participating Agencies, (ii) fully cooperate with other Participating Agencies to comply with applicable law concerning the Incident or Breach, including any notification to data subjects, and (iv) be liable for any expenses associated with the Incident or Breach including without limitation: (a) the cost of any required legal compliance (e.g., notices required by applicable law), and (b) the cost of providing two years of credit monitoring services or other assistance to affected consumers. In no event will the agency experiencing the Incident or Breach serve any notice of or otherwise publicize an Incident involving the Information detailed in this agreement without the prior written consent of all Participating Agencies.

8.3.3 Following notification of an Incident or Breach, the impacted agency must promptly provide all other Participating Agencies any documentation requested by those agencies, to complete an investigation, complete an investigation pursuant to the following requirements:

8.3.3.1 Make a determination as to whether a Incident or Breach occurred;

8.3.3.2 Assess the nature and scope of the Incident;

8.3.3.3 Identify Information that may have been involved in the Incident; and

8.3.3.4 Perform or oversee reasonable measures to restore the security of the Information compromised in the Incident to prevent further unauthorized acquisition, release, or use of the Information.

8.4. In the event of any conflict between the provisions of this Agreement and the attachments, the stricter of the conflicting provisions will control. If there is any ambiguity in the provisions of this agreement, the provisions hereof shall, at a minimum, be interpreted consistent with any state or federal law, or any contractual requirements applicable to Participating Agencies.

ARTICLE 9. GENERAL PROVISIONS

9.1. Ownership of Confidential information

Disclosing Agency is the owner of the information shared under this agreement. Any Receiving Agency who receives a request for public information related to such shared information must notify the Disclosing Agency within 5 business days, of acknowledgement of receipt of such request.

9.2. Certification

The participating agencies certify that:

9.2.1 They are authorized to engage in the exchange of data as described in the Scope of Information Exchange

9.2.2 The services or resources specified in this DEC are necessary and authorized for activities that are properly within the statutory functions and programs for each of the Participating Agencies;

9.2.3 The proposed arrangements serve the interest of efficient and economical administration of government

9.2.4 Any changes or updates to the terms of this agreement including the scope of information exchange shall be reflected in writing and approved by signing authorities prior to sharing data under the updated agreement.

9.3. Acceptable Use and Use Limitations

Data sharing under this agreement will be limited to the authorized purposes described herein, including the Scope of Information Exchange, consistent with the applicable legal authorities as defined.

9.3.1 **Limitations**

9.3.1.1 Data shared under this agreement shall not be used by Receiving Agency, or it's subcontractors, third parties, or any other authorized users for marketing purposes, except as expressed in this agreement.

9.3.1.2 Receiving Agency shall not use data for the sole benefit of the Receiving Agency or other third parties outside of the authorized purposes described in this agreement, and will not share, publish, sublicense, resell or disclose to third parties or publicly unless otherwise set forth in this agreement or as required by law.

9.3.2 **AI**

9.3.2.1 The Receiving Agency may not use the data under this agreement, as defined in the Scope of Information Exchange, in or with Automated Decision-Making Technology without express written agreement from the Disclosing Agency.

a) If personal data is included in the Scope of Information Exchange, such personal data may not be used by the Receiving Agency in or with an AI system without data subject consent. Such consent must be documented and align with applicable AI and Privacy Laws as detailed in the Scope of Information Exchange.

b) If consent is granted, the Receiving Party shall ensure that all Personal Data is first properly anonymized or de-identified in compliance with applicable law and subject to the Disclosing Party's written approval of the anonymization method.

c) Unless approved by the Disclosing Agency, information shared under this agreement may not be used to train public instances of AI systems.

9.3.3 **Personal Data**

Disclosing Agency agrees that Receiving Agency may collect, analyze and use data derived from Personal Data in de-identified form, in which all personally identifiable information, including direct and indirect identifiers, have been permanently removed or obscured so the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual ("De-Identified Data"), for the following purposes: (a) generating analyses and metrics whether alone or in combination with De-identified Data from other sources in aggregated and de-identified format (the "Analytical Results"); (b) providing Analytical Results and reports based on such Analytical Results to Disclosing Agency or other Participating Agencies under this agreement; (c) providing Analytical Results and reports to other stakeholders; (d) providing analytics and ongoing monitoring assessments to stakeholders; (e) developing and training Receiving Agency's predictive models or AI systems; and (f) conducting internal research, development, marketing and analytic purposes. Disclosing Agency agrees that Receiving Agency will have the right, both during and after the Term of this Agreement, to use, store, transmit, distribute, modify, copy, display, sublicense and create derivative works of the De-Identified Data.

9.4. Terms of Agreement

This agreement continues as long as the Participating Agencies have the requisite authority to enter into this agreement or until this agreement is terminated by all Participating Agencies. A Participating Agency may terminate its participation in the DEC with 30 days' notice to all Participating Agencies and the designated DEC Administrator or Disclosing Agency.

9.4.1 Participating Agencies will manage the DEC and any amendments. This DEC may not be amended without written agreement from all participants in the DEC.

9.4.2 Participating Agencies will manage the content of Attachment 1, Scope of Information Exchange.

By their signatures, the authorized representatives of the Participating Agencies bind their respective agencies to the terms set forth in this DEC.

In the event the authorized representative leaves one of the Participating Agencies, this agreement may be updated with a new designated signatory or authorized representative of the Participating Agency.

ARTICLE 10. INDEMNIFICATION

To the fullest extent allowed by law, Receiving Agency agrees to release, and defend (using legal counsel acceptable to the Disclosing Agency), indemnify, and hold harmless the Disclosing Agency, its departments, subsidiaries, affiliates and officers, officials, directors, employees, agents, representatives or volunteers, from any and all claims, losses, harm, costs, liabilities, damages and expenses (including attorney's fees) of any nature whatsoever, or allegations thereof, arising directly or indirectly out of Receiving Agency's use, transmission or disclosure of the Information, except to the extent that any such claims, losses, harm, costs, liabilities, damages and expenses are caused by the Disclosing Agency's negligence or willful misconduct. Receiving Agency expressly waives by mutual negotiation, all immunity and limitation of liability under any industrial insurance act, including [INSERT APPLICABLE STATE CODE HERE, E.G. TITLE 51 RCW], other Workers' Compensation Act, Disability Benefit Act, or other Employee Benefit Act of any jurisdiction, which would otherwise be applicable in the case of such claim.

PARTICIPATING AGENCY	**PARTICIPATING AGENCY**
BY: _____	**BY:**_____
NAME: _____	**NAME:**_____
TITLE: _____	**TITLE:**_____
DATE: _____	**DATE:**_____

ATTACHMENT 1. SCOPE OF INFORMATION EXCHANGE

This Scope of Information Exchange incorporates the specific terms and requirements of the [Organization] Data Exchange Compact (DEC) by reference. Both the Disclosing Agency and Receiving Agency identified in this Attachment each certify to being a Participating Agency to the DEC as of the date of the last party to sign this Scope of Information Exchange.

1. Disclosing Agency (or Agencies):
   _____
2. Receiving Agency (or Agencies):
   _____
3. Statutory authority for the disclosure: _____
4. Applicable policies and procedures documents:
   a. _____
   b. _____
5. Applicable laws and industry frameworks specific to this Scope:
   - [NIST 800-53]
   - [ISO 27001]
   - [Industry standards such as HIPAA, FERPA, CJIS, etc.]
   - [Insert applicable state privacy laws]
   - [Insert state public disclosure laws]
6. Oversight Agencies: _____
7. Authorized purpose for disclosure: _____
8. Authorized users: _____
9. Secure method of transmission and storage: _____
10. Frequency of exchange: _____
11. Volume of data: _____
12. Contact information for notices: [add more information if more than two agencies involved]
    a. Particpating Agency 1: _____
       i. Name:
       ii. Email:
       iii. Phone number:
    b. Particpating Agency 2: _____
       i. Name:
       ii. Email:
       iii. Phone number:

13. Data To Be Shared (Data fields, metadata, and other cataloguing information)

Records [RECEIVING AGENCY] will receive from [TRANSFERING AGENCY]		
Field Name	Variable	Notes

Disclosing Agency

Name: _____

Title: _____

Email: _____

Phone number: _____

Receiving Agency

Name: _____

Title: _____

Email: _____

Phone number: _____

14. Privacy/ Security Official: _____
15. Term of Agreement: _____
16. Agency-specific requirements: _____

    _____
17. Termination: _____
18. Fees/Costs: _____
19. Information & Data destruction requirements:

    ___[Destruction timeline; destruction method; timeframe requirement for reporting to Disclosing Agency]_____
20. Description of records, data, and information to be disclosed: [attach additional pages as necessary]

    _____

    _____

    _____
21. Purpose and Frequency of Notification:

    __[Breach; media coverage; send/received receipt notifications; data subject notification (as applicable), etc.]_____

DISCLOSING AGENCY

BY: _____

RECEIVING AGENCY

BY: _____

NAME: _____

TITLE: _____

DATE: _____

NAME: _____

TITLE: _____

DATE:_____

ATTACHMENT 2. DATA LEXICON

[INSERT APPLICABLE DATA LEXICON, IF NEEDED]