State of Arizona
Enterprise Data Sharing - Memorandum of Understanding

WHEREAS, the State of Arizona is committed to protecting the security of Data collected by the agencies, boards, commissions, and Budget Units of the State of Arizona who are signatories hereto (the "Partners"); and

WHEREAS, the State of Arizona complies with all Applicable Law related to Data security and privacy interests that may be associated with Data collected by the Partners; and

WHEREAS, to carry out their functions in the most expedient, efficient, and secure manner possible for the benefit of the citizens of the State of Arizona, it is necessary and appropriate for the Partners to securely exchange Data in accordance with Applicable Law; and

WHEREAS, the Partners frequently require the secure exchange of Data collected by other Partners to perform functions mandated by Applicable Law, to streamline business processes, and to maintain Data quality; and

WHEREAS, pursuant to A.R.S. § 18-104, the Arizona Department of Administration - Arizona Strategic Enterprise Technology Office ("ADOA-ASET") sets rules, policies, and standards related to information technology; and

WHEREAS, pursuant to A.R.S. § 18-105(C), the statewide information security and privacy office develops, implements, maintains, and ensures compliance by each Budget Unit with a coordinated statewide assurance plan for information security and privacy; and

WHEREAS, the Partners enter into this Enterprise Data Sharing Memorandum of Understanding ("EDS-MOU") to enable them to exchange Data in accordance with agreed terms and Applicable Law;

NOW, THEREFORE, for and in consideration of the mutual covenants contained herein, the Partners mutually agree to the provisions set forth in this EDS-MOU.

1) DEFINITIONS

For the purposes of this EDS-MOU, the following terms shall have the meaning ascribed to them below.

A) "Applicable Law" shall mean all Federal and Arizona laws and regulations applicable in the context of a given Data Exchange.

B) "Authorization" shall have the meaning and include the requirements set forth at 45 CFR § 164.508 and any similar Applicable Laws with additional requirements.

C) “Breach” shall mean all known incidents that result in the unauthorized access, use, or disclosure of Data protected by federal or state laws.

D) “Budget Unit” shall have the meaning set forth in A.R.S. § 18-101.

E) “Data” shall mean information in any form that refers to, represents or describes entities such as conditions, ideas, objects, persons, events, transactions, and for the purposes of this agreement, includes personal, confidential, private and public Data.

F) “Data Exchange” shall mean a specific instance or case of Data Sharing.

G) “Data Exchange Service” shall mean any System that serves to exchange Data between Partners.

H) “Data Request” shall mean a request for Data made by one Partner to another.

I) “Data Sharing” shall mean the exchange of Data or information between two entities by any means.

J) “Data Sharing Agreement” or “DSA” shall refer to a contractual agreement between two or more partners delineating the terms and conditions of a specific Data Exchange.

K) “Data Transmittal” shall mean an electronic exchange of Data between Partners using agreed upon Specifications.

L) “Designated Representative” shall mean the individual chosen by a Partner to be responsible for all communications related to this EDS-MOU between that Partner and other Partners.

M) “Discloser” shall mean a Partner that discloses Data to another Partner through a Data Transmittal in any format.

N) “Dispute” shall mean any controversy or disagreement arising out of, or relating to, this EDS-MOU.

O) “Effective Date” shall mean the date of execution of this EDS-MOU by a given Partner.

P) “Emergent Specifications” shall mean new technical Specifications that existing and/or potential Partners are considering to implement to test the feasibility of emerging technology, to identify whether the Specifications reflect an appropriate capability for the Partners, and assess whether the Specifications are sufficient to add as a production capability available to the Partners.

Q) “Information Technology Service Provider” or “ITSP” shall mean an organization that provides a Partner with operational, technical, cloud or other information technology services.

R) “Interoperability” has the same meaning as provided in P4440.

S) “Notice” shall mean a communication sent to the Designated Representative of a Partner in accordance with this EDS-MOU.

T) “Partner” shall mean an agency, board, commission or Budget Unit of the State of Arizona that is a signatory to this EDS-MOU, and includes an ITSP or contractor working specifically for a Partner.

U) “Personally Identifiable Information” or “PII” is information which can be used on its own or in combination with other information to identify a specific individual.

V) “Recipient” shall mean the Partner and any other person or entity that receives or has access to the Data through a Data Transmittal from a Discloser pursuant to this EDS-MOU.

W) “Re-Identification” shall mean the reverse engineering of events or Data elements for the purpose of permitting an individual to be uniquely identified after Data has been de-identified.

X) “Specification” shall mean the provisions established by Applicable Law or adopted by the SDIC that prescribe the Data content, technical, and security requirements needed to enable the Partners to Transmit Data. Specifications may include, but are not limited to, specific standards, services, and policies applicable to Data Transmittal pursuant to this EDS-MOU.

Y) “Subject Person” shall mean a natural person whose Data is maintained by a Partner and is subject to exchange with another Partner.

Z) “System” shall mean the software, portal, platform, or other electronic medium controlled by a Partner through which the Partner conducts its Data Transmittal related activities. For purposes of this definition, it shall not matter whether the Partner controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

AA) “Transmit”, “Transmittal”, or “Transmitting” shall mean, in varying tenses, to send Data electronically using the Specifications.

BB) “User” shall mean any employee or contractor of a Partner who has been authorized to access the Data.

2) PRINCIPLES

A) The following Statewide Information Security Policies ("Security Policies") and Standards ("Standards"), which may be amended from time to time, are incorporated herein by reference and the Partners hereby acknowledge their responsibility to comply with these Security Policies and Standards as then in effect:

a) National Institute of Standards and Technology (NIST) SP800-53 R4
b) Arizona Baseline Infrastructure Security Controls
c) P8110 Data Classification Policy
d) P8120 Information Security Program Policy
e) S8120 Information Security Program Standard
f) P8130 System Security Acquisition and Development Policy
g) P8210 Security Awareness and Training Policy
h) S8210 Security Awareness Training and Education Standard
i) P8220 System Security Maintenance Policy
j) S8220 System Security Maintenance Standard
k) P8230 Contingency Planning Policy
l) P8240 Incident Response Planning Policy
m) S8240 Incident Response Planning Standard
n) P8250 Media Protection Policy
o) S8250 Media Protection Standard
p) P8260 Physical Security Protections Policy
q) P8270 Personnel Security Controls Policy
r) P8280 Acceptable Use Policy
s) P8310 Account Management Policy
t) P8320 Access Controls Policy
u) S8320 Access Controls Standard
v) P8330 System Security Audit Policy
w) S8330 System Security Audit Standard
x) P8340 Identification and Authentication Policy
y) S8340 Identification and Authentication Standard
z) P8350 System and Communication Protections Policy
aa) S8350 System and Communication Protections Standard
bb) P8410 System Privacy Policy

B) The following Statewide Data Governance Policies ("Data Governance Policies"), which may be amended from time to time, are incorporated herein by reference and the Partners hereby acknowledge their responsibility to comply with these Data Governance Policies as then in effect:
a) P4400 Data Governance Organization Policy
b) P4430 Data Governance Technology Policy
c) P4440 Data Governance Data Interoperability Policy
d) P4470 Data Governance Documentation Policy

C) The purposes of this EDS-MOU are:

a) To facilitate Interoperability of Data between the Partners; and
b) To enable Partners to exchange information with other Partners upon request, to facilitate such exchanges, remove barriers to such exchanges, and provide a governance framework to determine how Data Sharing occurs between Partners.

D) The Partners hereby agree to the overarching principle that any and all Data in their custody may be shared within their agency and with another Partners for a valid purpose unless at least one of the following is true:
a) A contractual agreement with a third party explicitly prohibits sharing it with another Partner; or
b) Sharing of the specific Data is prohibited by Applicable Law; or
c) Sharing of the specific Data would negatively impact operational or safety activities.

E) A contractual agreement or Applicable Law that restricts the manner in which Data is shared, restricts specific Data elements that may be shared, or restricts re-sharing of the Data shall not be deemed to be a blanket prohibition from sharing the Data set.

F) The Partners agree that Re-Identification of Obfuscated or De-Identified PII is not permissible and will take steps to train personnel and implement countermeasures to prevent this from happening.

G) Each Partner shall comply with State Data Security and Privacy policies, Applicable Law, this EDS-MOU, and all applicable Specifications in Transmittal of Data.

3) STATE DATA INTEROPERABILITY COUNCIL

A) The Partners hereby agree to form a State Data Interoperability Council ("SDIC").

B) The SDIC shall be comprised of one member from each of the Partners. If the Partner has established a Data Policy Council in accordance with Policy P4400 (Data Governance Organization Policy) then that body shall elect a member to the SDIC.

C) The SDIC shall be chaired ("Chairperson") by the State Chief Data Officer, if one has been appointed, or a person designated by the State Chief Information Officer ("SCIO").

D) Motions shall be passed by a simple majority of the members present and voting.

E) A quorum is comprised of one third of the registered members who are present in-person, telephonically, or through video conference.

F) Members may send a proxy to attend and vote on SDIC items in their absence.

G) The SDIC shall schedule regular meetings not less than quarterly, or more frequently as necessary or at the call of the Chairperson or designee.

H) The SDIC shall be responsible for the following:
   a) Supporting secure Data Transmittal;
   b) Maintaining a list of all EDS-MOU Partners, their Designated Representative(s) and their preferred contact information, which shall be made available to all EDS-MOU Partners;
   c) Mediating Disputes between Partners with legal and compliance issues;
   d) Advising the SCIO or designee as to how to resolve Disputes between Partners in accordance with this EDS-MOU;
   e) Managing amendments to this EDS-MOU; and
   f) Fulfilling other responsibilities related to Data Interoperability delegated by the SCIO or designee to the SDIC.

I) Mediation Process for Disputes A Partner may request that the Chairperson convene a special meeting of the SDIC for purposes of mediating a dispute with another Partner(s) related to Data Sharing. If the Chairperson grants such a request, a special meeting of the SDIC shall be scheduled as soon as practicable. When holding a special meeting for purposes of mediating a dispute between Partners, members of the SDIC may provide non-binding recommendations as to how the Partners in dispute should proceed toward a resolution.

4) USE OF DATA

A) Partners shall Request and Transmit Data in accordance with Applicable Law. Partners shall enforce this provision and the DSA with its Users, employees, vendors and any other person or entity that receives, sends, or has access to Data pursuant to this EDS-MOU.

B) Recipients shall retain and use Data in accordance with Applicable Law, the DSA and the Recipient’s record retention policies and procedures.

C) Recipients shall not disclose Data to any outside entity or person, including subcontractors, unless such disclosure is explicitly permitted in the DSA.

D) Each Partner certifies that unless permitted or required to share Data by Applicable Law, it has obtained a Uniform Authorization to Exchange Information (UAEI), which permits it to disclose Data for the Subject Person served by the Partner for whom an inquiry is made pursuant to this EDS-MOU. If the Partner does not have a signed UAEI, but has a previously signed Authorization in a different form, the previous Authorization may be sufficient until the UAEI is signed. Such Authorization may be included as part of the Subject Person’s application form or it may be a separate consent to release form, which shall be kept in the Subject Person’s file. In either case, the Subject Person must sign the Authorization, or where the Subject Person is a minor, the Subject Person’s parent or legal guardian. If the Subject Person has a representative authorized to act on his or her behalf, the representative may sign the release.

5) EXPECTATIONS, DUTIES, AND RESPONSIBILITIES OF PARTNERS

A) All Partners shall collaborate with other Partners and shall respond to a Data Request from another Partner in the affirmative, unless specifically prohibited in accordance with Paragraph 2D. [Amended 8-15-2019]

B) A Partner making a Data Request shall submit the request to the Designated Representative of the Partner from which the requested Data originates, who shall provide a response approving or denying the Data Request within ten (10) business days by either:

a) Requesting, in writing, a one-time extension of the time to approve or deny the request by no more than 10 additional days,
b) Approving, the Data Request in writing, or
c) Providing a written denial of the Data Request, accompanied by a statement explaining the specific legal authority requiring the denial.
d) Partners may agree to further extensions of the time to respond not to exceed 45 days in total from the date of the request. In the event that the responding Partner requires additional time to respond, the Parties may agree to extend the time further to avoid a denial. [Amended 8-15-2019]

C) If the Data Transmission to Partners is specifically prohibited by Applicable Law or by operational or security concerns, Partners shall work to identify if any edits, deletions or additional protections can be made to comply with Applicable Law and allow Data to be provided to a Partner.

D) Each Partner shall be responsible for maintaining a secure environment compliant with State security policies, standards and guidelines, and other Applicable Law.

E) Partners shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by the DSA and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Data. Appropriate safeguards shall be those required by Applicable Law and the State Data Security and Privacy Policies and Standards.

F) Each Partner agrees to have written privacy and security policies, including Access and Disclosure Policies, in place before the Partner’s Effective Date, meeting State Security Policies based on NIST 800-53 rev. 4.

G) Each Partner agrees to employ security controls so that Data Transmittal will not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, malware or Data designed to disrupt the proper operation of a System or defeat any State or Partner security controls.

H) Agreements with Users. Each Partner shall have established agreements with each of its Users that require the User to, at a minimum:

a) Comply with all Applicable Law;
b) Cooperate with Partners on issues, tasks and requests related to this EDS-MOU;
c) Transmit Data only for a permitted purpose;
d) Use and disclose Data received from another Partner or User only in accordance with the terms and conditions of this EDS-MOU;
e) Within 24 hours after determining that a Breach occurred, User will report such Breach to the SCIO or designee and the State's CISO, and follow the Partner's internal reporting procedures;
f) Refrain from disclosing to any other person any passwords or other security measures issued to the User by the Partner;
g) Sign the User Acknowledgement form found in Attachment D; and
h) Cooperate with any external audits.
i) With respect to Users who are employed by a Partner or who have agreements with the Partner which became effective prior to the Effective Date, compliance with this Section may be satisfied through written policies and procedures that address items (a) through (h) of this Section.

I) Agreements with Vendors. To the extent that a Partner uses vendors in connection with the Partner's Transmittal of Data, each Partner affirms that it has established agreements with each of its vendors, including ITSPs, that require the vendor to, at a minimum:
a) Comply with Applicable Law;
b) Protect the privacy and security of any Data to which it has access;
c) As soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Partner;
d) Not to re-disclose information without written consent of the Partner;
e) Use information only for the purposes for which it was made available under the Business Purposes provided in the Specifications;
f) Agree to the same restrictions on the access, use, and disclosure of Data as contained herein;
g) Cooperate with the other Partners to this EDS-MOU on issues, tasks and requests related to this EDS-MOU;
h) Sign the User Acknowledgement form found in Attachment D; and
i) Cooperate with any external audits.

J) Upon termination of a Data Exchange Service the Recipient shall:
a) Transfer Data back to the Discloser and take any additional steps specified in the DSA and Specifications;
b) Purge all Data in its possession, including all Data residing on computer hardware, cloud services, magnetic or optical media and paper. This purge shall be performed in the manner set forth in the requirements for "Purge" contained in NIST SP800-88, Appendix A: Minimum Sanitization Recommendation for Media Containing Data."

6) TERM OF THE AGREEMENT; ADDITION OF PARTNERS

A) This Agreement will take effect upon execution and will remain in full force and effect perpetually throughout the existence of the Partners, unless terminated by Statute or Rule.

B) If a Partner is transferred, subsumed or merged with another State Budget Unit by Statute, Rule or Executive Order then the successor Budget Unit shall remain bound by the terms of this agreement unless such statute or order specifically prohibits it.

C) Agencies, boards, commissions, and Budget Units of the State of Arizona may request to join this EDS-MOU and become a Partner.

D) When an Applicant requests to join this EDS-MOU, the request shall be directed to the Chairperson of the SDIC in writing. The SDIC shall review the request to ensure it conforms to the requirements of the EDS-MOU.

E) The Chairperson shall place the approval of the Application on the agenda of the next scheduled SDIC meeting.

F) If the SDIC approves the Application, the Applicant shall execute this EDS-MOU and assume all the obligations and privileges of a Partner.

G) The Chairperson of the SDIC shall forward the approval of the new Partner to the SCIO or designee, the new Partner's Designated Representative, and Chief Executive Officer.

H) If the SDIC does not approve the Applicant's request to become an EDS-MOU Partner, the SDIC will so advise the Applicant, with specific reasoning as to why they are precluded from participation.

7) PROCESS TO AMEND THE EDS-MOU

A) Any Partner may submit in writing to the SDIC Chairperson a request for an amendment to the EDS-MOU. All requests for proposed amendments shall identify:

a) The section of the EDS-MOU that is the subject of the requested amendment;
b) A description of why the requested amendment is desired;
c) The proposed language for the requested amendment; and
d) An analysis of the expected impact of the requested amendment.

B) Upon receipt of a request for amendment the SDIC Chairperson shall place the item for consideration on the agenda for an upcoming meeting.

C) Members may vote to defer consideration of an amendment to a future meeting if it requires further deliberation or study. [Amended 8-15-2019]

D) The Amendment shall be approved by a ⅔ vote of the members present and voting. [Amended 8-15-2019]

E) If the SDIC approves the amendment, the SDIC Chairperson shall forward the amended text to all members. [Amended 8-15-2019]

F) A member who objects to the amendment may submit a new request for amendment to the Chairperson, or, at their option, may withdraw from the Memorandum of Understanding. [Amended 8-15-2019]

G) EDS-MOU Signatories hereby delegate authority to their designated agency representatives to act on their behalf in this amendment process. [Amended 8-15-2019]

8) INITIATING NEW DATA EXCHANGE, DATA SHARING AGREEMENT AND SPECIFICATIONS

The DSA shall articulate the following details with respect to the specific Data being exchanged, either in the body of the DSA or in attachments referenced within the DSA:

A) The business purpose of the Data Exchange;

B) Applicable Law that permits or mandates the Data Exchange;

C) Applicable Law that restricts the use of the Data being exchanged in any way;

D) Permitted use of the Data;

E) Permitted retention period of the Data;

F) Steps to take at the expiration of the retention period to destroy or return Data to the Discloser;

G) Permitted sharing of the Data with third parties;

H) An explanation as to whether an existing Interoperability standard is being applied, such as an internal standard, HL7, NIEM, etc. If the Data service does not follow an approved standard, or there is no standard, specify this as well.

I) An evaluation of whether additional Partner-specific restrictions should be applied on the Data Exchange. User or Group level restrictions shall be included, if applicable.

J) The Privacy Classification of the Data, which defines special security considerations to be applied to a Data element. Examples include:

- PII – Personally Identifiable Information
- PHI – Protected Health Information
- MH/BH – PHI with additional protections – treat as mental/behavioral health Data
- PCI – Payment Card Industry

- SSA – Treat as SSN content under Arizona and federal legislation
- EDUCATION – Treat as educational Data, subject to FERPA (Family Educational Rights and Privacy Act)
- SUBSTANCE ABUSE – PHI with additional protections – treat as substance abuse information under federal law

K) The technical Specifications for the Data, including:
  a) Data elements and description of each;
  b) File format (CSV, Tab, flat, XML, JSON, etc.)
  c) Required metadata such as row count, file totals, layout version, privacy indicators, etc.
  d) Reference Data version and last update identifiers (ICD10, CPT, etc.)
  e) List of valid values for internal reference Data (department, division, agency, etc.)
  f) How to identify changed rows;
  g) Data types;
  h) Precision of numeric and GIS Data;
  i) Special formatting – identifies special formatting that should be applied to the field content by the Partner consuming the service. Example patterns include:
    - (###) – field value must be numeric up to 999.
    - (###.##) – field value must be numeric up to 999 and allows 2 digits of decimal precision
    - (0) – field value must be between 0 and 9; zero will be treated as a default
    - ($##.####) – field value must be up to $99.99; fractional parts of a dollar will preserve ten and one digits by retaining a zero.
    - (MM/DD/YYYY) – field value will be treated as a multi-part date field
    - (APPROVED|REJECTED|PENDED) – field value must be one of the allowed values listed.

L) The Service Level Agreement for Data deliveries (Data available by 4AM, etc.). If the Data Exchange is mission-critical and requires high availability, this shall be stated in the Agreement;

M) Frequency and schedule of transmission (weekly, 1st Thursday of each month, etc.);

N) Period of time covered by each transmission (full replacement, last 7 days transactions, etc.);

O) Delivery mechanism (FTP/SFTP pull/push, web service, API, etc.);

P) A process for restarting the service should the transfer fail unexpectedly;

Q) Test procedures and pass/fail criteria;

R) Details on the Data transfer process, including:
  a) Tracing the business path of the Data transfer from the source System to the target location;

b) Identifying if any updates or transformations are made to the Data in transit;
c) Capturing details on the transport protocol that will be applied transferring the Data;
d) Noting if the transport protocol changes along the path; and
e) Indicating the transfer/transmittal protection requirements to ensure the Data content is protected appropriately per Applicable Law.

S) Starting and ending dates;

T) The time period in which the Data remains valid and relevant;

U) Any requirements for citations of the Data and credit for its use;

V) Any disclaimers required on reports and other artifacts generated from the Data;

W) Validation routines that will ensure that message format and content are valid and that content has been received without error;

X) A statement from the Discloser that describes the fitness for use of the Data, or a disclaimer that they are not responsible for the fitness for use;

Y) Source of the Data – identify where the Data originated from, to help the user understand how to interpret the Data values, how to protect the Data and how the Data can be used. Example sources include:
a) Citizen –was provided by a Citizen or User
b) Partner – sourced from a State Agency, either active or inactive with the Exchange
c) 3rd party –is provided by an external third party entity, not affiliated with any state Agency
d) SSA – field content came from the Social Security Administration
e) IRS – field content came from the Internal Revenue Service
f) CMS - field content came from the Centers for Medicare and Medicaid Services;

Z) The Origin of the Data, which serves to clarify the applicable business functions allowed with the Data content and further defines the source of the Data including the System, application and Data field which were the source of the content; and

AA) A feedback mechanism to report erroneous Data back to the Discloser for correction and reprocessing.

9) MISCELLANEOUS

A) Notices. All Notices to be made under this EDS-MOU shall be given in writing to the authorized Partner's representative at the address listed with the SDIC, and shall be deemed given:

a) Upon delivery, if personally delivered or through the State's inter-agency mail service;
b) Upon the date indicated on the return receipt, when sent by the United States Postal Service Certified Mail, return receipt requested; and
c) If by electronic Transmittal, upon the date and time of sending the Notice is directed to an electronic mail address listed with the SDIC.

B) Governing Law. This EDS-MOU shall be governed by and construed in accordance with the laws of the State of Arizona.

C) Amendment. This EDS-MOU may be amended as provided herein. All Partners agree to sign any amendment duly adopted in accordance with this EDS-MOU.

D) Entire EDS-MOU. This EDS-MOU, together with all Appendices and Attachments, constitutes the entire agreement. The official, executed version of this EDS-MOU shall be maintained in an electronic form by the SCIO or designee. The SCIO or designee shall maintain the EDS-MOU is a format that is accessible to all EDS-MOU Partners.

E) Validity of Provisions. In the event that any Section, or any part or portion of any Section of this EDS-MOU, is determined to be invalid, void or otherwise unenforceable, each and every remaining Section or part or portion thereof shall remain in full force and effect.

F) Priority. In the event of any conflict or inconsistency between a provision in the body of this EDS-MOU and any attachment hereto, the terms contained in the body of this EDS-MOU shall prevail.

G) Headings. The headings throughout this EDS-MOU are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify, or aid in the interpretation or construction of meaning of the provisions of this EDS-MOU. All references in this instrument to designated "Sections" and other subdivisions are to the designated Sections and other subdivisions of this EDS-MOU. The words "herein," "hereof," "hereunder," and other words of similar import refer to this EDS-MOU as a whole and not to any particular Section or other subdivision.

H) Relationship of the Partners. Nothing in this EDS-MOU shall be construed to create a partnership, agency relationship, or joint venture among the Partners. Neither the SDIC nor any Partner shall have any authority to bind or make commitments on behalf of another Partner for any purpose, nor shall any such Partner hold itself out as having such authority. No Partner shall be held liable for the acts or omissions of another Partner.

I) Effective Date. With respect to the first two Partners to this EDS-MOU, the Effective Date shall be the date on which the second Partner executes this EDS-MOU. For all

Partners thereafter, the Effective Date shall be the date that the Partner executes this EDS-MOU.

J) Counterparts. This EDS-MOU may be executed in any number of counterparts, each of which shall be deemed an original as against the Partner whose signature appears thereon, but all of which taken together shall constitute one and the same instrument.

K) Third-Party Beneficiaries. There shall exist no right of any person to claim a beneficial interest in this EDS-MOU or any rights occurring by virtue of this EDS-MOU.

L) Force Majeure. A Partner shall not be deemed in violation of any provision of this EDS-MOU if it is prevented from performing any of its obligations by reason of:
   a) severe weather and storms;
   b) earthquakes or other disruptive natural occurrences;
   c) power failures;
   d) nuclear or other civil or military emergencies;
   e) terrorist attacks;
   f) acts of legislative, judicial, executive, or administrative authorities; or
   g) any other circumstances that are not within its reasonable control. This Section shall not apply to obligations imposed under Applicable Law.

M) Time Periods. Any of the time periods specified in this EDS-MOU may be changed pursuant to the mutual written consent of the SCIO and the affected Partner(s).

N) Ownership. Any Data provided by a Discloser to a Recipient shall remain the property of the Discloser even after it is provided to a Recipient. Recipient shall not obtain any right, title, or interest in the Data.

O) Court Order or Subpoena. In the event that any Data is required to be disclosed in response to a valid order to a court of competent jurisdiction or other governmental body of the United States or any political subdivisions thereof, only the minimal necessary Data shall be disclosed to the extent necessary and for the purposes of the court or other governmental body. The Partner will be notified of the order as soon as practicable and provided with a copy of such order as soon as practicable and Partner may seek a protective order.

P) Public Notification. If required by Applicable Law, Partner will post a copy of this EDS-MOU for public access.

IN WITNESS WHEREOF, the undersigned authorized representatives have caused this Agreement to be executed.

Name	Position	Agency	Signature	Date
Bill Boyd	Deputy Director	Department of Forestry and Fire Management		
Gilbert Davidson	Chief Operating Officer and Interim Director	Arizona Department of Administration	[Signature on file]	
Mark Killian	Director	Arizona Department of Agriculture	[Signature on file]	
Gregory McKay	Director	Arizona Department of Child Safety	[Signature on file]	
Michael Trailor	Director	Arizona Department of Economic Security	[Signature on file]	
Robert D. Charlton	Director	Arizona Department of Financial Institutions	[Signature on file]	
James Ashley	Interim Director	Arizona Department of Gaming	[Signature on file]	
Gilbert M. Orrantia	Director	Arizona Department of Homeland Security	[Signature on file]	
Keith A Schraad	Interim Director	Arizona Department of Insurance	[Signature on file]	
Jeff Hood	Director	Arizona Department of Juvenile Corrections		
Col. Frank Milstead	Director	Arizona Department of Public Safety	[Signature on file]	
Judy Lowe	Commissioner	Arizona Department of Real Estate		
John S. Halikowski	Director	Arizona Department of Transportation	[Signature on file]	
Wanda Wright	Director	Arizona Department of Veterans' Services	[Signature on file]	
Thomas Buschatzke	Director	Arizona Department of Water Resources	[Signature on file]	
Ty E. Gray	Director	Arizona Game and Fish Department	[Signature on file]	
Thomas J. Betlach	Director	Arizona Health Care Cost Containment System	[Signature on file]	
Gregory Edgar	Executive Director	Arizona Lottery	[Signature on file]	

Name	Position	Agency	Signature	Date
Debbie Johnson	Director	Arizona Office of Tourism	[Signature on file]	
Jeff Fleetham	Director	Arizona Registrar of Contractors	[Signature on file]	
Carlton Woodruff	Interim Director	Department of Revenue	[Signature on file]	
Lisa A. Atkins	Commissioner	Arizona State Land Department	[Signature on file]	
Charles Ryan	Director	Department of Corrections	[Signature on file]	
Major General Michael T. McGuire	Director	Department of Emergency and Military Affairs		
Misael Cabrera	Director	Department of Environmental Quality	[Signature on file]	
Dr. Cara Christ	Director	Department of Health Services		
Carol Ditmore	Director	Department of Housing	[Signature on file]	
Alberto Gutier	Director	Governor's Office of Highway Safety	[Signature on file]	
Sandra Watson	Interim Director	Office of Economic Opportunity	[Signature on file]	
Maria Cristina Fuentes	Director	Governor's Office of Youth, Faith and Family	[Signature on file]	
James Ashley	Director	Industrial Commission of Arizona	[Signature on file]	
David Tenney	Director	Residential Utility Consumer Office	[Signature on file]	

Name	Position	Agency	Signature	Date
Andy LeFevre	Executive Director	Arizona Criminal Justice Commission	[Signature on file]	

AMENDMENT HISTORY

August 15, 2019

Amendment 1:

Strike Paragraphs 7C through 7G

~~Q) If the SDIC determines that the request does not have merit, it shall communicate this determination to the requesting Partner.~~

~~R) If the SDIC determines that the request has merit, the SDIC shall forward the request to the SCIO or designee to seek approval of the recommended amendment. When the SDIC seeks approval of such amendments, the SDIC shall provide the SCIO or designee with the following information:~~

~~a) A copy of the proposed amendment to the EDS-MOU;~~
~~b) Description of why the requested amendment is desired and any foreseeable impact of the amendment;~~
~~c) Statement regarding whether the proposed amendment is necessary in order for the SDIC or Partners to comply with Applicable Law; and~~
~~d) Projected date on which the proposed amendment will take effect.~~

~~S) If the SCIO or designee agrees with the proposed amendments to the EDS-MOU, the SCIO or designee will advise all of the Partners of such decision and the date on which the proposed amendment will take effect.~~

~~T) The SDIC shall meet to vote on recommending proposed amendments to the EDS-MOU. For proposed amendments to be recommended by the SDIC, at least two-thirds of the members of the SDIC must approve the amendment.~~

~~U) Once an amendment is recommended by the SDIC, and the SCIO agrees with the recommendation, all Partners are advised to sign the amendment to the EDS-MOU prior to the date on which the amendment takes effect.~~

and insert the following:

C) Members may vote to defer consideration of an amendment to a future meeting if it requires further deliberation or study.
D) The Amendment shall be approved by a ⅔ vote of the members present and voting.
E) If the SDIC approves the amendment, the SDIC Chairperson shall forward the amended text to all members.
F) A member who objects to the amendment may submit a new request for amendment to the Chairperson, or, at their option, may withdraw from the Memorandum of Understanding.
G) EDS-MOU Signatories hereby delegate authority to their designated agency representatives to act on their behalf in this amendment process.

Amendment 2:

Paragraph 5A

A) All Partners shall collaborate with other Partners and shall respond to a Data Request from another Partner in the affirmative, unless specifically prohibited by Applicable Law.

Is amended to read as follows:

5A) All Partners shall collaborate with other Partners and shall respond to a Data Request from another Partner in the affirmative, unless specifically prohibited in accordance with Paragraph 2D.

Amendment 3:

Paragraph 5B is amended to add the following paragraph:

d) Partners may agree to further extensions of the time to respond not to exceed 45 days in total from the date of the request. In the event that the responding Partner requires additional time to respond, the Parties may agree to extend the time further to avoid a denial.