ARIZONA DEPARTMENT OF ECONOMIC SECURITY
Information Risk Management
3443 North Central, Mail Drop 1426, Phoenix, Arizona 85012
Phone: (602) 771-2676 | Fax: (602) 364-0481

DATA SHARING REQUEST/AGREEMENT

BETWEEN

REQUESTING ENTITY:

DES Division/Administration/Program/Office Name or External Organization Name:

_____

AND

DATA MANAGER: ARIZONA DEPARTMENT OF ECONOMIC SECURITY

Division/Administration/Program/Office Name:

_____

DSA Effective Date: _____ **DSA Agreement No.:** _____

Contract Start Date: _____ **Contract No.:** _____

Contract Max End Date: _____ **UID:** _____
(If applicable)

Agreement No. _____

SECTION I. REQUEST *(Completed by Requesting Entity)*
Use attachment if necessary

1a. PURPOSE OF THIS REQUEST *(What information is being requested and why? How will it be used? Define business need. Give details/specifics.)*

1b. INFORMATION TECHNOLOGY AND CONNECTIVITY TYPE *(VPN, DVD, Citrix, Mainframe, etc.; or some other alternative way of accessing application/data?)* ***Select all approriate and explain in detail below:***

☐ Citrix ☐ VPN-Client ☐ MainFrame ☐ Secure-FTP ☐ Secure-Email ☐ Other

1c. INFORMATION TYPE BEING ACCESSED *(Personal Identifiable Information, FBI, SSA, HIPAA , define)*

1d. WILL THIS INFORMATION BE RETAINED?

◯ Yes ◯ No If Yes, where and how?

PLEASE SELECT THE TYPE OF INFORMATION REQUESTED AND SPECIFIC FIELDS:

☐ HIPAA ☐ PCI ☐ PHI ☐ PII ☐ Full Name ☐ Home Address
☐ SSN or National Identification Number ☐ Vehicle Registration Plate ☐ Driver's License Number
☐ Fingerprints ☐ Credit Card Numbers ☐ Digital Identity ☐ Date of Birth
☐ Birth Place ☐ Gender/Race ☐ Heath/Medical Records ☐ Wage/Tax Info.
☐ Phone Number ☐ Criminal Record ☐ Medical Benefits Eligibility Records

The requester enters all information required for successful communication between the requesting entity and the DES IT Staff.

Contact Name (1): _____ Phone: _____

Contact Name (2): _____ Phone: _____

Contact Address: _____

Contact (1) E-Mail Address: _____

Contact (2) E-Mail Address: _____

Contact Fax No: _____

Agreement No. _____

SECTION I. (Cont.) REQUEST *(Completed by Requesting Entity)*
Use attachment if necessary

2. CITE LAW, REGULATION, DIRECTIVE OR OTHER BASIS FOR THIS REQUEST

3. WILL OTHER ENTITIES INTERFACE/WORK WITH YOUR ORGANIZATION?
◯ Yes ◯ No If Yes, identify entity and reason(s):

4. WILL INFORMATION BE DISCLOSED/SHARED WITH ANOTHER ENTITY/ORGANIZATION?
◯ Yes ◯ No If Yes, identify the entity/organization and reason(s) for disclosure:

5. WILL DES DATA BE STORED IN ANY FORM OF (DATABASES, FILES, TAPES, PAPER COPYS, ETC.)? WILL DATA BELONGING TO DES BE STORED IN A SECURE SPECIFIED ON-SITE LOCATION?
◯ Yes ◯ No If Yes, identify where, what type of data and how the data is to be stored, and for how long?

6. WHAT ARE THE SAFEGUARDS IN PLACE TO GUARD AGAINST UNAUTHORIZED ACCESS/DISCLOSURE OF THE INFORMATION; ACCESS CONTROL PARAMETERS, ROLE BASED ACCESS, ETC.

☐ Computers and stored in secure ☐ Encryption ☐ Secure Physical Location ☐ Locked File Cabinet
☐ 8 Characters or more Password Location ☐ Role based Access Permissions/Need to know

6a. IF AN INFORMATION BREACH SHOULD OCCUR, WHAT ARE YOUR PROCESSES AND PROCEDURES TO ADDRESS THIS? (SEE SECTION 2, #6)

7. HOW WILL THE INFORMATION BE PRESENTED FOR USE? WILL THE INFORMATION BE POSTED, DIGITALLY COPIED, APPLICATION, ETC?

8. HOW WILL THIS INFORMATION BE DISPOSED OF WHEN NO LONGER NEEDED? SEE RETENTION POLICY.

Print Name and Title of Authorized Contact: _____

Phone: _____ Fax: _____ E-mail: _____ Date: _____

Mailing Address/Mail Drop: _____

City: _____ State: _____ ZIP Code: _____

Agreement No. _____

SECTION II. STIPULATIONS REGARDING THE USE OF INFORMATION

STIPULATIONS APPLICABLE TO THE REQUESTING ENTITY:

1. Disclosure of the data provided to the Requesting Entity is not permitted unless specifically authorized.
2. Repackaging or redistribution of data or screens, or creation of separate files will not be permitted unless specifically authorized.
3. The data shall be used only to assist in legal valid business needs as stated in Section I, item 1a of this Agreement.
4. All data shall be stored in a physically secure logically encrypted facility/system following the physical security regulations and standards based on the type of data appropriate and related standards. HIPAA / PHI / PII / PCI/ PUB-1075 etc.
5. All data in electronic format shall be safeguarded and stored, processed and monitored so that unauthorized persons cannot compromise the information.
6. DES shall be notified within 24 hours when an information breach occurs. Notification must be in accordance with timelines based on State and Federal law.
7. Only authorized staff will be given access to accomplish the purpose(s) specified in Section I, item 1a of this Agreement.
8. Staff shall view, read or attend an authorized data security awareness training class, where they will be instructed on confidentiality, privacy laws and penalties imposed when there in any non compliance. All staff with access to DES systems and/or applications must complete an annual recertification security awareness training class as scheduled by DES.
9. A Request for Terminal Access and/or other Activity (J 125) shall be used to request specific access for each authorized staff member and must be signed by the staff supervisor or designee.
10. All authorized staff are required to sign a User Affirmation Statement (J 129), as a condition for using requested data. This affirmation statement must be resigned at three (3) year intervals as scheduled by DES.
11. Any changes requiring additional access or removal of access as, shall be reported promptly to the respective data security analyst.
12. Federal and state audit and data security personnel may have access to offices and records of the requesting entity to monitor or verify compliance with this Agreement.
13. This Data Sharing Agreement will remain in effect for 10 years from the effective date unless otherwise stipulated in Section III or overridden by the Contract, a Memorandum of Understanding or an InterAgency Agreement. If duration is overridden by another document, please reference the document in Section III.
14. Upon Contract Termination, Media Sanitization procedures shall be adhered to in accordance to Arizona Statewide Policy – P8250v 1.0 - The Business Unit shall sanitize digital and non-digital information system media containing Confidential information prior to disposal, release of organizational control, or release for reuse using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250. [NIST 800-53 MP-6] [HIPAA 164.310(d)(2)(i)] [HIPAA 164.310(d)(2)(ii)] [IRS Pub 1075]
15. All DES Contracts retention terms and conditions will be adhered to as written unless otherwise stated on DES Retention Policy [(DES 1-37-12-(01)(02)(03)] is applicable.
16. Requesting entity is responsible for all costs and licenses associated with securely connecting to DES and for maintaining confidential standards.

STIPULATIONS APPLICABLE TO PROVIDER:

1. DES will use the Requesting Entity employee identifying information solely for the purpose of establishing access.
2. Only authorized DES employees will have access to requesting agency employee data.
3. In accordance with applicable federal, state, and/or local privacy regulations, DES will protect all information collected from the Requesting Entity.

STIPULATIONS APPLICABLE TO HIPAA – HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

1. All staff shall attend an authorized HIPAA awareness training class, where they will be instructed on confidentiality, privacy, information safeguards and penalties imposed when compliance is breached.
2. If applicable, a “Business Associate Contract” [45 CFR 164.502(e), 154.504(e). 164.532(d) & (e)] on file and it will be attached to this data sharing agreement as an addendum.

STIPULATIONS APPLICABLE TO DIVISION DATA OWNERS:

1. DES Division Security Rep shall verify external or internal requesters and submit service desk ticket (SD) and attach the received **(J-125 from external customers only)** and process account. SD ticket must contain DSA# and all contents of attached J-125 in the SD summary field. DES Division Security Reps shall monitor and manage all accounts which have access to their data or with who this DSA in partnership.

Agreement No. _____

SECTION III. ADDITIONAL INFORMATION

TERMINATION OF AGREEMENT ONLY:

a. Information will be returned based on Contract terms and conditions. ◯ Yes ◯ No

b. Information will be truncated (erased/deleted). ◯ Yes ◯ No

c. Information in physical form shall be shredded. ◯ Yes ◯ No

d. All of the above. ◯ Yes ◯ No

External Agency POC (Print Name): _____ Phone Number: _____

Signature: _____ Date: _____

SECTION IV (A). RECOMMENDATIONS
(Completed by the Data Managing Program/DATA OWNER)

☐ Recommend **APPROVAL**

☐ Request is not recommended for approval

Print Name: _____ Phone Number: _____ Date: _____

Signature: _____ Mail Drop: _____

SECTION IV (B). PRIVACY RECOMMENDATIONS
(Completed by the division HIPAA or PRIVACY OFFICER)

☐ Recommend **APPROVAL**

☐ Request is not recommended for approval

Print Name: _____ Phone Number: _____ Date: _____

Signature: _____ Mail Drop: _____

SECTION IV (C). DES ENTERPRISE SERVICE DELIVERY
(Completed by DTS SERVICE DELIVERY MANAGER)

☐ Recommend **APPROVAL**

☐ Request is not recommended for approval

Print Name: _____ Phone Number: _____ Date: _____

Signature: _____ Mail Drop: _____

Agreement No. _____

SECTION V. APPROVAL
(Completed by the requesting entity and the data managing program)

I attest to the correctness of the information provided in Section I and agree to the stipulations and costs if any listed in Section III. I agree to comply with all provisions of the DES Data Security Policy. If any violations of the DES Data Security Policy occur, this Agreement may be terminated. I further understand that DES will periodically review the terms of the Agreement to ensure it conforms with DES Policies and Procedures. In the event changes in either federal or state law or regulations occur that conflict with the terms of the Agreement or render the terms of the Agreement void, impracticable, or otherwise impossible, this Agreement will terminate immediately. A new Agreement or an amendment to the existing Agreement will be initiated to provide for any changes that cannot be accommodated within the provisions of the existing Agreement. The Requesting Entity shall hold harmless and indemnify the State of Arizona and its Department of Economic Security for any liability resulting from acts or omissions attributable to the Requesting Entity.

IN WITNESS HERETO, the PARTIES have executed this Agreement by signature of their duly authorized officials:

FOR THE REQUESTING ENTITY: *(Completed by requesting Entity)*

Entity Name: _____

Print Signatory Name: _____ Title: _____

Signature: _____ Date: _____

FOR THE DEPARTMENT OF ECONOMIC SECURITY: *(Completed by Data Managing Program)*

Entity Name: _____

Print Signatory Name: _____ Title: _____

Signature: _____ Date: _____

SECTION VI. APPROVAL
(Completed by Information Risk Management)

This signed Agreement meets all requirements necessary to permit the controlled sharing of the DES data while simultaneously providing for the protection of the data. I certify that:

☐ **THIS AGREEMENT CONFORMS TO DES Information Security Policy [DES 1-38-0006].**

☐ **THIS AGREEMENT DOES NOT CONFORM to the DES Information Security Policy. Implementation of this agreement cannot proceed until the following action is taken:**

_____	**DES Chief Information Security Officer**	_____
(Signature)	*(Title)*	*(Date)*

ROUTING INSTRUCTIONS FOR J-119

DATA- SHARING AGREEMENT BETWEEN DES ENTITIES:

1. Section I, II and III are completed, contact information is provided and the document is signed by the requesting Division or Program Assistant Director, Program Administrator, or designee. The requesting entity Division or Program Security Analyst sends the document to the Data Managing Division/Program Security Analyst. The DSA/PSA from the Data Managing Division/Program will complete Section III and the recommendation in Section IV. If applicable, the Division HIPAA Privacy Officer will complete the recommendation in Section IV. Reason must be given if request is not recommended for approval. Section V is signed and dated by the Data Managing Assistant Director, Program Administrator or designee.

EXCEPTION: All DERS UI Data Sharing Agreements will follow their own established process.

2. The data managing Division/Program Security Analyst forwards the Agreement to the Enterprise Delivery Team for signature and approval of Information technology connectivity. Enterprise service delivery team sends DSA back to the Division/Program security team for final signatures. The Agreement is signed, and dated by the Information Security Administrator. The original Agreement is sent back to the Division/Program entered into the tracking list. The Agreement is scanned PDF to the network share, for all data sharing agreements. DSA is not final until fully signed by all parties.

NOTE: When the Agreement is modified during the approval process, both entities must review the modifications and re-sign/date the document.

DATA-SHARING AGREEMENT BETWEEN DES AND AN EXTERNAL ENTITY:

1. Section I, II and III are completed by the requesting entity, contact information is provided and the document is signed by the requesting entity and Division or Program Assistant Director, Program Administrator, or designee. The Division or Program Security Analyst sends the document out for signatures. If applicable, the Division HIPAA Privacy Officer will complete the recommendation in Section IV. Reason must be given if request is not recommended for approval. Section V is signed and dated by the requesting entity administrator and Data Managing Assistant Director, Program Administrator or designee.

EXCEPTION: All DERS UI Data Sharing Agreements will follow their own established process.

2. The data managing Division/Program Security Analyst forwards the Agreement to the Enterprise Delivery Team for signature and approval of Informaton technology connectivity. Enterprise service delivery team sends DSA back to the Division/Program security team for final signatures. The Agreement is signed, and dated by the Information Security Administrator. The original Agreement is sent back to the Division/Program entered into the tracking list. The Agreement is scanned PDF to the network share, for all data sharing agreements. DSA is not final until fully signed by all parties.

NOTE: When the Agreement is modified during the approval process, both entities must review the modifications and re-sign/date the document.

DATA SHARING AGREEMENT WITH INTERNAL (if applicable) EXTERNAL CONTRACTS BETWEEN ENTITIES PROCEDURES: STEP BY STEP

1. From the Contracts Division for which the Contract has been originally created, the authorized Contracts person shall contact the Security Representative from the specific Agency for which the Contract was created, notify that a Data Sharing Agreement (DSA) is needed and being requested and a copy must be sent to the Security Representative to start the process of creating a DSA.
   a. **NOTE: A DSA request will not be honored without a valid Contract (number) (if applicable) accompanying the DSA.**

2. Any external Contracts agreed upon by DES that include the sharing of information require a J-119 – Data Sharing Agreement (DSA). The normal longevity of the J-119 DSA is 10 years. The newly agreed upon Contract terms and conditions supersedes the longevity of the DSA length of 10 years to align with the Contracts terms, conditions, and longevity.
   a. Example: If a newly accepted Contract of 2 years needs a DSA, the DSA will align with the Contracts longevity of 2 years. A DSA is created.
   b. If at the end of the 2 years the contract is renewed for 1 more year, then the contract's personnel shall inform the Agency's Security Team of the contract extension. Agency's Security Team will update the DSA tracking database to reflect the contract extension. The DSA can be renewed every year(s) up to 10 years (the total life-cycle of a DSA) before a new DSA is created.

      i. J-119A (Amendment Form) is required when additional access to other information not stipulated in the original DSA is being requested. For any extensions/changes of a DSA along with the following requirements:
         1. J-119A must document the changes to the original DSA.
         2. J-119A must document the new Contract Number.
         3. Document any and all changes made on the renewed Contract that involve terms and conditions in the sharing of information.
         4. Assign an agreement number to the DSA and put the Contract number on the first page of the DSA (preferably typed).
         5. DSA with other hand written notes, directions, alterations and scratch offs will not be accepted by IRM.
         6. Security Representative will enter all data into the DSA Database and will select status field "pending signatures to IRM."

      Words of CAUTION:
      a. Security Representative that has created the DSA will have to reproduce the DSA once again to be compliant, no exceptions.
      b. A DSA that is attached to a Contract will not be approved by IRM without a valid contract number.

3. When the Security Representative has completed all the applicable/signatures, the DSA agreement is enterd into the Data Security Warehouse Database by the Security Representative with a status of "Pending-IRM Approval." Afterwards the DSA agreement is sent to IRM, to DES Information Security Administrator, 1720 W. Madison St., Phoenix, AZ 85007 (Site Code 829Z), for final review and approval. The agreement is then signed and dated by the Information Security Administrator.

4. The original agreement is filed in the DES Data Managing Division/Program and the IRM Security Representative confirms all data in the DSA database. The Agreement is not final until signed by the IRM Security Representative, the DES Executor, and the Requesting Entity(s).

5. A final digital copy of all signatures of essential personnel mentioned above is required to IRM for IRM Security Administrator to change the DSA to ACTIVE with in the database.