**DATA USE AGREEMENT**

**Drafting Notes:**

1. Fill in all blanks and then remove the blank lines.
2. Certain insertions are highlighted in yellow. After completing insertion, remove language in yellow.
3. Delete Drafting Notes from your final document.

This Data Use Agreement (“Agreement”) is executed on this \_\_\_\_ day of\_\_\_(Month), 20\_\_\_\_ (“Execution Date”), to be effective on the \_\_\_\_ day of \_\_\_\_(Month), 20\_\_\_\_, (“Effective Date”), by and between the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Agency”) and \_\_\_\_(insert requesting organization’s name) (“Data Requestor”), by \_\_\_\_(name of individual from organization making the request) its \_\_\_\_(insert title of signatory). Unless extended pursuant to section 5.2, this Agreement will terminate on \_\_\_\_ (insert Month X, 20xx)**.**

**R E C I T A L S**

**WHEREAS,** this Agreement supersedes all previous agreements or contracts between the Data Requestor and the Agency:

**WHEREAS,** the Agency is the record owner and maintains the Data Set (described in Section 2.3 below). (Insert description and statutory authority);

**WHEREAS,** the Agency agrees to disclose a Data Set, as defined herein, to the Data Requestor for use by Data Requestor in the performance of certain functions (“Activities”, described Section 2.2 below); and,

**WHEREAS,** the Data Requestor agrees to limit its use of the Data Set and protect it according to the terms and conditions of this Agreement.

**NOW THEREFORE,** in consideration of the mutual agreements, covenants, terms and conditions herein contained, the Agency and the Data Requestor agree as follows:

**I. DEFINITIONS FOR USE IN THIS AGREEMENT**

“Data Security” shall mean the technical, physical, and administrative controls applied and implemented to safeguard data and protect the unauthorized access to the Data Set(s).

“Disclosure” shall mean the release, transfer, access to or divulging of information in any other manner outside the entity holding the information.

“Electronic Media”shall mean the mode of electronic transmissions. It includes the Secure File Transfer Protocol Site, Internet, Intranet, extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, private networks, and those transmission that are physically moved from one location to another using portable storage media, including but not limited to: removable magnetic media, including external hard disk drives, external devices containing hard disk drives, and magnetic tape; rewritable DVDs or CDs portable USB-based flash drives, also known as thumb drives, jump drives, or key drives; memory cards such as SD, CompactFlash, Memory Stick or any related flash-based supplemental storage media; portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function; PDAs, cell phones, and Smartphones with internal flash or hard drive-based memory that support a data storage function; and, digital cameras with internal or external memory support.

**“**Personally Identifiable Information” or “PII” shall mean all information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes all subcategories, such as Protected Health Information, and Federal Tax Information, and cardholder data regulated by the Payment Card Industry Data Security Standards.

“Record” shall mean any item, collection, or grouping of data about an individual(s) that is maintained, collected, received, used or disseminated by the Agency.

**II. PURPOSE**

**Section 2.1 Purpose.**

The Data Requestor seeks the data for the purposes delineated in Exhibit “A”, which is a copy of the executed Data Request Form.

**Section 2.2 Activities.**

The Data Requestor seeks to perform specified activities with the data as delineated in Exhibit “A”.

**Section 2.3 Data Set.**

The Data Requestor agrees to use and the Agency agrees to disclose the following Data Set, with the variables delineated in Exhibit “B”, to the Data Requestor for use by the Data Requestor in the performance of the Activities described above.

**III. OBLIGATIONS OF THE DATA REQUESTOR**

**Section 3.1. Use of Data Set.**

The Data Requestor shall use the Data Set only as permitted under the terms of this Agreement, and any additional terms from the data request or letter of intent, or required by law, but shall not otherwise use the Data Set and shall ensure that its governing body, employees, contractors and agents do not use the Data Set in a manner that would constitute a violation of this Agreement. The Data Requestor may not use any information provided hereunder for any purpose not listed in this Agreement without prior written approval of the Agency. The Data Requestor agrees not to use the Data Set in such a way as to identify any individual and further agrees not to contact any individual whose information is found within the Data Set. The Data Requestor agrees that it will limit use of the Data Set to the minimum number of individuals necessary to achieve the Activities outlined above. The Data Requestor shall limit the use or disclosure of the Data Set to the individuals set forth in Exhibit “C” and shall identify, in this same exhibit, one person with whom the Agency may contact regarding this agreement. To the extent that this list changes, the Data Requestor will provide a supplementary list to the Agency fifteen (15) business days in advance of the proposed disclosure, for Agency’s approval.

**Section 3.2. Disclosure of Data Set.**

The Data Requestor may disclose the Data Set only as permitted under the terms of this Agreement. In a report, the Data Requestor will not present statistics with direct identifiers, or with indirect identifiers with cell sizes less than or equal to 10. The Data Requestor will not in any manner, directly or indirectly, make known, disclose, publish or communicate the Data Set itself, or any part thereof, including but not limited to derivatives, to any person, firm, or corporation without the express written consent of the Agency. (OPTIONAL: If you want electronic copies, remove this yellow highlighting and instructional parenthetical. If you do not want electronic copies, remove the language highlighted in yellow in its entirety.) Upon request, the Data Requestor will provide electronic copies of any reports and publications utilizing the Data Set to the Agency.

**Section 3.3. Safeguards against Misuse of Information.**

The Data Requestor shall use appropriate and reasonable safeguards to prevent use or disclosure of the Data Set other than as permitted under this Agreement. The Data Requestor shall make audit reports available upon the Agency’s request. The Agency or its designee may conduct audits of Data Requestor’s security, including requesting a copy of the most current security policy, or a copy of the Institutional Review Board approval or waiver. The Data Requestor shall maintain and not alter the Data Set’s values, thus ensuring integrity.

**Section 3.4. Reporting of Unauthorized Disclosures of Information.**

The Data Requestor shall, as quickly as possible, but no later than twenty-four (24) hours of becoming aware of any use or disclosure of the Data Set in violation of the Agreement by the Data Requestor, its governing body, employees, contractors or agents or by a third party to which the Data Requestor disclosed the Data Set pursuant to 3.2, report any such disclosure to the Agency. Such notice shall be emailed to the attention of the \_\_\_\_ (insert Agency) Privacy Officer, \_\_\_\_ (insert Agency Privacy Officer’s email address). Such disclosure shall also be reported to the Agency at the following phone number \_\_\_\_ (insert Agency’s primary phone number).

**Section 3.5. Security Administrator Designation.**

The Data Requestor will provide the name, title and telephone number of its designated Security Administrator, as well as a photo copy of the Administrator’s state issued driver’s license or other government-issued photo identification, to the Agency before any records are accessed. The Security Administrator will be responsible for access and use of any Agency records. The Security Administrator will also be responsible for requesting log-on identification numbers from the Agency, to the extent this is applicable, and to whom the Agency may provide log-on identification numbers. The Security Administrator is responsible for the security of all log-on identification numbers assigned to the Data Requestor and will ensure that the assigned log-on identification numbers and passwords are not exchanged or shared with any other person(s) or entities. If the Security Administrator or any employee of the Data Requestor leaves the employ of Data Requestor or changes job duties and no longer requires access to Agency records as part of their official job assignments, the Security Administrator will immediately notify the Agency, which will cancel the access log-on code for the employee. Within 30 calendar days of separation or transfer, the Security Administrator will notify the Agency of any authorized user(s) who no longer needs access to Agency records and may make a request to authorize a new log-on access number.

**Section 3.6. Agreements by Third Parties.**

The Data Requestor shall obtain and maintain an agreement with each agent or subcontractor that has or will have access to the Data Set, which is received by or on behalf of the Data Requestor. The agent or subcontractor shall agree to be bound by substantively the same restrictions, terms, and conditions that apply to the Data Requestor pursuant to this Agreement with respect to the Data Set. Special restrictions, terms and conditions, if any, may be found in Exhibit “D”. Prior to any disclosure to a third party, the Data Requestor must obtain the written consent of the Agency in conformity with Section 3.2 of this Agreement.

**Section 3.7 Notice of Request for Data.**

The Data Requestor agrees to notify the Agency within five (5) business days of the Data Requestor’s receipt of any request, including a freedom of information request, or subpoena for the Data Set. The Data Requestor shall not release information prior to the Agency’s response to Data Requestor’s notification. To the extent that the Agency decides to assume responsibility for challenging the validity of such request, the Data Requestor shall cooperate fully with the Agency in such challenge.

**Section 3.8 Indemnification.**

To the extent allowable by law, the Data Requestor shall indemnify, defend (if requested by the Agency), and hold the Agency harmless from and against any actual or threatened legal or administrative action, claim, liability, penalty, fine, assessment, lawsuit, litigation, or other loss, expense or damage, including without limitation any reasonable attorney’s fees and costs that the Agency may incur directly or indirectly resulting from any action or omissions of the Data Requestor, its agents, subcontractors, including failure to perform its obligations under this Agreement, without regard to any limitation or exclusion of damages provision otherwise set forth in this Agreement.

**Section 3.9 Injunction.**

The Data Requestor acknowledges and agrees that the Agency will suffer irreparable damage upon the Data Requestor’s breach of this Agreement and that such damages shall be difficult to quantify. The Data Requestor acknowledges and agrees that the Agency may file an action for an injunction to enforce the terms of this Agreement against the Data Requestor, in addition to any other remedy the Agency may have.

**Section 3.10. Ownership of the Information.**

The Data Requestor acknowledges that, as between the Data Requestor and the Agency, all data contained in the Data Set shall be and remain the sole property of the Agency, including any and all forms thereof developed by the Data Requestor in the course of its fulfillment of its obligations pursuant to the Agreement.

**IV. TERMINATION**

**Section 4.1 Termination Upon Breach.**

In the event that the Data Requestor, its governing body, employees, contractors or agents, or a third party to which the Data Requestor disclosed the Data Set pursuant to 3.2, breaches any provision contained in this Agreement, the Data Requestor, upon Agency approval, may attempt to cure. If such breach is not cured within a five (5) business day period, the Data Requestor has a duty to discontinue use and disclosure of the Data Set and to report the breach to the Agency, notwithstanding any other provision of this Agreement to the contrary. Due to Data Requestor’s breach, the Agency may, at its sole discretion, terminate this Agreement upon five (5) business days written notice to the Data Requestor.

**Section 4.2 Return or Destruction of Information upon Termination.**

Upon termination of this Agreement, the Data Requestor shall either return or destroy all data contained in the Data Set received from the Agency or created or maintained in any form. (Optional: Specific destruction standards may be found in Exhibit D.) If the data is destroyed, the Data Requestor must submit the following with certification by two people within the organization: the date of the destruction, the means used to destroy the data and confirmation that the destruction complied with applicable standards. The Data Requestor shall not retain any copies of such data, or its derivatives. The Agency or its designee may conduct audits of Data Requestor’s destruction. Notwithstanding the foregoing, to the extent that the Agency agrees that it is not feasible to return or destroy such data, and any derivatives, the Data Requestor will continue to be bound by the terms of this Agreement as long as the Data Requestor retains the Data Set, in any form.

**V. GENERAL PROVISIONS**

**Section 5.1 Effect.**

The terms and provisions of this Agreement, including any amendments or attachments, constitute the complete agreement and shall supersede any other conflicting or inconsistent agreement between Agency and Data Requestor.

**Section 5.2 Amendment.**

The Data Requestor and the Agency may amend this Agreement, upon joint, written agreement of both parties. Additionally, the parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Agreement.

**Section 5.3 Governing Law.**

The Agreement shall be governed by the laws of the State of West Virginia.

**Section 5.4 No Third-Party Beneficiaries.**

Nothing express or implied in this Agreement is intended to confer upon any person other than Agency, Data Requestor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

**IN WITNESS WHEREOF**, the parties have caused this Agreement to be executed as of the day and year first written above.

|  |  |  |
| --- | --- | --- |
| **(Insert Agency’s Name)** |  | **(Insert Data Requestor’s Organization’s Name)** |
| **By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **(Insert Agency Representative’s Name)** |  | **By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **(Insert Data Requestor Representative’s Name)** |
| **Its: (Insert title)** |  | **Its: (Insert title)** |
| **Date:** |  | **Date:** |

Exhibit A

(Insert a copy of the executed Data Request Form.)

Exhibit B

(Insert a description of the Data Set to be released, identifying all variables and including relevant supporting documentation.)

Exhibit C

(Insert list of individuals accessing data including name, title, organization and address.)

Exhibit D

(Insert any specific terms and conditions here.)

(Optional Destruction Specifications)

Paper, film, or other hard copy media have been shredded or destroyed such that the personally identifiable information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

Electronic media have been cleared, purged, or destroyed consistent with National Institute of Standards and Technology “NIST” Special Publication 800-88, Guidelines for Media Sanitization, such that the personally identifiable information cannot be retrieved. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>