Public Safety Policy and Research Center
Office of Financial Management

TRIP Data Governance Manual

TRAFFIC RECORDS INTEGRATION PROGRAM

About TRIP

The Washington State Traffic Records Integration Program (TRIP) is a data integration program housed within the Office of Financial Management's Public Safety and Research Policy Center and is funded by a grant through the Washington Traffic Safety Commission. TRIP works with various state agencies to collect and integrate data related to motor-vehicle collisions. The purpose of the TRIP program is to develop and maintain a data repository for public health and safety research to further the goals of the Washinton's Target Zero plan to achieve zero fatalities or serious injuries on Washington roadways.

Contact Us

Phone	Fax	Address	Email
360-902-0555	360-586-1988	P.O. Box 43113 Olympia, WA 98504-3113	trip@ofm.wa.gov

Acknowledgements

This program would not be possible without the help and support of the Washington Traffic Safety Commission (WTSC) and our data contributors – the Washington State Department of Transportation (WSDOT), Washington Department of Licensing (DOL), Washington State Patrol (WSP) – toxicology laboratories, Washington Administrative Office of the Courts (AOC), and Washington Department of Health (DOH).

This document and the program and processes would not have been possible without the help and support of OFM's Education Research and Data Center (ERDC). Many of these policies and procedures have been directly adapted from ERDC efforts.

Version History

Date	Version	Author(s)	Revision Note
07/01/2023	1.0	Ian Kinder-Pyle, MS	Document creation
02/01/2024	1.1	Ian Kinder-Pyle, MS	Annual Update
05/09/2025	1.2	Vasiliki Georgoulas-Sherry, PhD, Ian Kinder-Pyle, MS and Trevor Annis, MS	Annual Update

Table of Contents

Introduction

Purpose

This document describes the OFM's TRIP data governance structure and processes to assess and review data requests from both external and internal sources. The TRIP is dedicated to protecting stakeholders and preventing the disclosure of private data and information. By successfully engaging in this process, the TRIP can mitigate the adverse effects of poor data quality, while promoting effective data management.

For more information on program history including mission and vision please review the TRIP's Program Manual.

Data Governance & Data Security Overview

Data Governance and Data Security are two interconnected, yet distinct programs that ensure the privacy and safekeeping of data that enters and leaves the TRIP repository. Data governance is the framework that defines how the data is managed, ensuring it is accurate, consistent, and used responsibly. Data security focuses on protecting that data from unauthorized access, breaches, or loss through tools like encryption and access controls.

Data Governance for the TRIP is documented through:

1. **Business & Technical Processes:** The TRIP business processes ensure compliance with regulatory requirements in state and federal policies, and within the various data sharing agreements and data requests that the TRIP engages in in terms of proper access, use, and storage of data. Technical processes are followed to ensure accurate, timely, and pertinent data analysis to help maintain limited access and the safe exchange of data with contributors and requestors.
2. **People Roles:** Our governance ensures that staff meet professional standards for privacy and data use, that we involve our data contributors, and we maintain trusting relationships with informed data requestors.

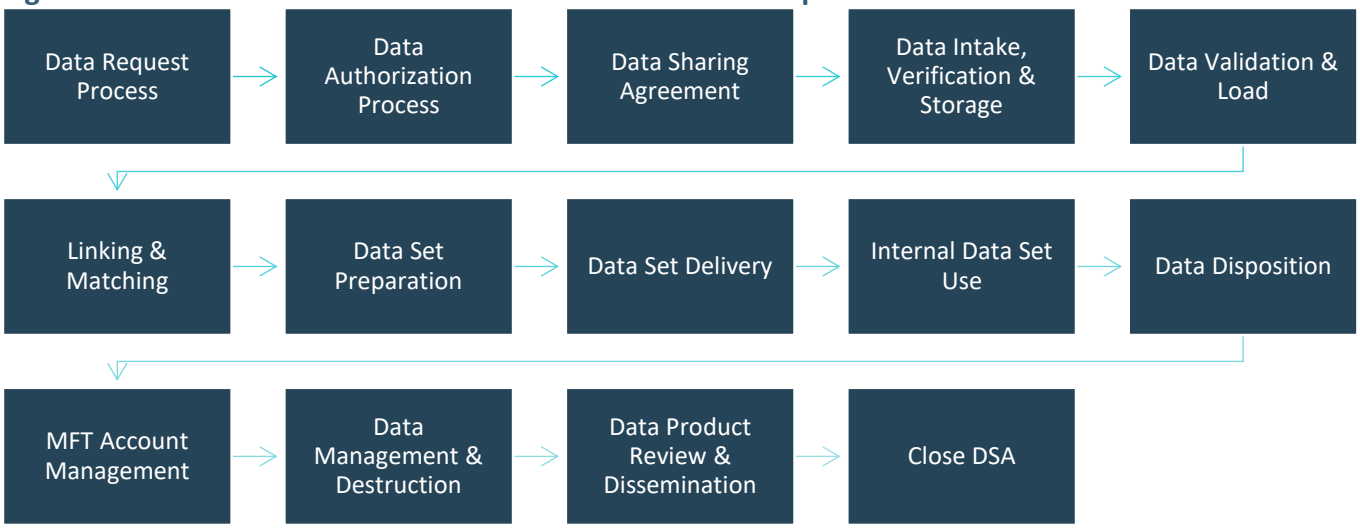
Data Security for the TRIP is documented through:

1. **Business & Technical Processes:** Our business processes are designed to ensure the security of data as it moves from the TRIP partners to the TRIP, as it resides within the TRIP repository, as it moves on to data requestors. This includes safeguards to protect TRIP's physical and electronic data assets from unauthorized access or misuse.
2. **People Roles:** The TRIP staff and contractors who access and/or work with either the data or system or both in a research or technical capacity operate in a manner that precludes inappropriate data access.

Data Governance and Data Movement Process Map

The TRIP's business processes are performed with the goal of providing data products to requestors and maintaining and safeguarding data within the repository. This document describes the data governance processes (see Figure 1).

Figure 1: Data Governance and Data Movement Process Map



Data Access

Data access to the TRIP is limited to analysts and researchers following approval from data contributors and the WSIRB.

Data Minimization

Data minimization ensures that only relevant data is collected and shared, aligning with policies that promote responsible data use. This reduces the risk of unauthorized access, improves data quality, and supports compliance with legal and ethical standards.

Data Privacy and Confidentiality

Data supplied to requestors from the TRIP repository is limited to de-identified data. Personally identifiable information (PII) will not be shared, and the TRIP protects individual data contained in the repository from unauthorized access, misuse, or disclosure, and ensures compliance with legal and ethical standards.

Data Destruction

At the end of each research project, data must be destroyed and purged from the applicable system(s). Additionally, a data destruction form will be completed, signed, and provided to the TRIP to confirm the destruction of the necessary data.

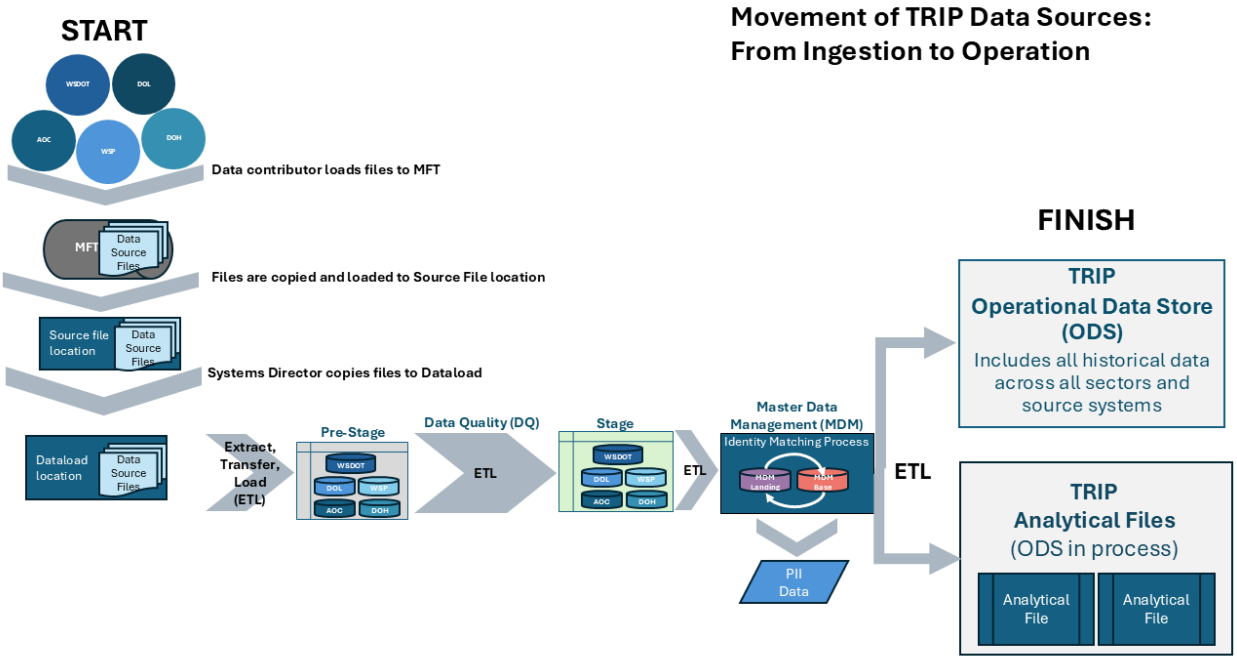
Data Flow Process

Figure 2 illustrates the data flow and loading process for the TRIP. The process includes:

(1) following retrieval of the source data, completing an initial data profile (e.g., did we get what we were expecting, are counts accurate),
(2) updating extract, transform, and load (ETL) routines if necessary (e.g., new fields, new codes) and loading it into the Pre-Stage environment (i.e., environment used to receive, clean, and prepare raw data before it is loaded into the main staging or data warehouse layers),
(3) loading to Stage environment (i.e., environment where raw or semi-processed data is placed before it undergoes further transformations and is loaded into the final data warehouse for analysis and reporting),
(4) loading to Master Data Management (MDM) environment (i.e., the framework which performs identity resolution within and between datasets),
(5) and loading to Operational Data Store (ODS) environment (i.e., environment consisting of a centralized database designed to integrate and store data from the different source systems).

The TRIP staff organize the source data and centralize the loading function. Throughout the loading process the TRIP staff update data readiness documents, source-to-target mappings, valid value tables, data deletion, data loading status, code promotion logs, and data intake logs.

Figure 2: Flowchart of data through stages of the TRIP loading process



Data Contributor Roles & Opportunities

Several organizations contribute data to the TRIP. The TRIP signs a data sharing agreement with each agency that outlines several components, including but not limited to the purpose of sharing data with the TRIP, data access, security, and disposition, as well as language regarding redisclosures. Data sharing agreements are discussed in more detail in a later section.

Currently, TRIP receives data from the Washington State Department of Transportation (WSDOT), Washington Department of Licensing (DOL), Washington State Patrol (WSP), Administrative Office of the Courts (AOC), and Department of Health (DOH). For more information about the data, please review the TRIP's Data Handbook.

The TRIP hosts a quarterly gathering for all state agency partners that share data with the TRIP for use. There are three primary purposes of this group:

1. To create a space for agencies to collaborate on research priorities.
2. To create a space for agencies to share legislative priorities and updates.
3. To keep the TRIP data contributors informed about the TRIP updates related to research and data governance; as well as keep the TRIP informed about topics important to data contributors.

The TRIP asks that data contributing agencies:

- Act as subject matter experts for domain-specific data
- Ensure the stability of the technology solution by:
    - Communicating to the TRIP with sufficient time, changes in data structure or format.
    - Communicating internal business technology changes which could affect the delivery of data to the TRIP system.
- Review the TRIP products and products created by data requestors.
- Provide quality assured data.
- Provide a data dictionary.
- Attend Data Contributor's Group meetings on a regular basis.

TRIP is implemented via a grant through the Washington Traffic Safety Commission (WTSC). As a subgrantee, TRIP receives oversight from the WTSC - WTSC plays a critical role in the TRIP by overseeing the collection, integration, and analysis of traffic safety data. The WTSC works to improve traffic safety in Washington State by leveraging data-driven strategies and ensuring the accurate reporting of traffic-related incidents. This includes data integration and coordination, stakeholder collaboration, funding and resource allocation, and supporting analysis and reporting.

Privacy Overview

TRIP adheres to OFM's privacy program, as well as a set of more specific privacy principles. OFM's privacy program moves the idea of privacy into a culture of privacy by identifying our compliance obligations associated with data, combining those compliance obligations with best practices, and then aligning OFM policy and internal controls to reflect a high level of data stewardship in the protection of confidential information. A privacy program gives us a framework for managing privacy-related issues consistently by creating policies and procedures at a functional level, hence, reducing risk and building trust. OFM's privacy program is built with a broad base of support throughout OFM's division to work on development and implementation of the privacy program. OFM Forecasting and Research currently has three privacy champions. Privacy Champions help facilitate awareness of privacy principles and their application to collecting, handling and disseminating OFM's confidential information. They also assist in the creation, review, monitoring and implementation of OFM's Privacy Program. This includes carrying out OFM's policies and procedures related to the privacy and security of confidential information.

The following privacy principles were adopted as OFM Policy #4.01 Privacy Program:

Security

We protect the confidential information entrusted to us against unauthorized access. Confidential Information is specific information that is not disclosable or is made confidential by law or for which special handling is required.

Minimization/Purpose Driven

We limit the collection, access, and use of confidential information to only what we require to provide OFM services and retain it only as long as necessary to meet our business needs and legal requirements.

Transparency

We are transparent about what confidential information we collect, why we collect it, and how it is used.

Accountability

We are accountable for collecting, using, managing, and disposing of confidential information in a manner that is consistent with best practices and as required by law, OFM policies and procedures.

Value Driven

We are respectful of privacy rights associated with confidential information entrusted to us.

Culture Driven

We will ensure that OFM staff have access to relevant privacy training, resources, and guidance.

Due Diligence/Lawful Use

We only share confidential information consistent with the law and under an OFM agreement. Agreements shall include instructions about how confidential information is protected. For public records, we shall apply all applicable exemptions before sharing records containing confidential information. For all confidential information shared, we shall apply data minimization principles and redactions as possible.

Privacy Principles and Considerations

The TRIP values the protection of privacy for all people and is guided by the following privacy priorities:

Lawful, fair & responsible use

The TRIP data collection, use, and disclosure is based on legal authority. The TRIP collects, uses, and discloses information responsibly and ethically, avoiding discrimination, deception, or harm. The TRIP follows privacy laws to safeguard the confidentiality of data. The TRIP's privacy practices are also guided by Office of the Chief Information Officer (OCIO) Policy 141.10 and the Washington State Agency Privacy Principles. Additionally, per Revised Code of Washington (RCW) 42.48, the WSIRB is responsible for providing the requisite regulatory review, approval and oversight of research that may involve these state agencies' clients, beneficiaries, patients, wards and state agency employees or these individuals' state agency personal records, in order to ensure the protection of the rights and welfare of human subjects of research. The TRIP implements this by complying with state and federal guidelines such as OCIO Policy 141.10 and RCW 42.48.

Data Minimization

The TRIP collects, uses, or discloses the minimum amount of information to accomplish the stated purpose for collecting the information. The TRIP implements this by collecting only data that is essential for research related to improving traffic safety, crash analysis, and public health.

Small Number Standards

The TRIP respects and honors the data that is included in the TRIP repository. The TRIP implements this by following small numbers standards[1] in data reporting suppressing all non-zero counts which are less than ten.

Transparency & Accountability

The TRIP strives for both transparency and accountability. Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances. Accountability means being responsible and answerable for following data privacy laws and principles. The TRIP implements this by ensuring that data processes, policies, and decision-making are clearly documented and available to research partners, committees, and oversight entities, as appropriate.

Due Diligence

The TRIP takes reasonable steps and exercises care before and after entering into data use agreements with state agencies and third parties that include sharing personal information.

Security

The TRIP uses appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, availability, and control of personal information. The TRIP implements this through a combination of policies, technologies, and procedures designed to protect sensitive crash and crash-related data from unauthorized access, breaches, and misuse.

[1] Hodge, Jr. JG, Piatt JL, White EN. Washington State Public Health Data Sharing Law & Policy Review: Final Report. Washington State Department of Health, Olympia, WA: 2024: 1-56 WA DOH PH Data Legal Rpt FINAL.pdf

Data Request Process

The TRIP was created to be an authoritative and comprehensive data repository, accessible by internal and external researcher entities for the purpose of increasing understanding of how various traffic-related variables influence collision outcomes in Washington. This section provides information on how data requests from outside entities should be managed.

The TRIP data repository is open to the public which can be requested for research use, upon approval by the WSIRB and the data contributors, if necessary. Data requested through the TRIP may not be used for-profit research.

Request Data

All requestors, regardless of their role or agency, must follow this request process:

1. Plan your data request.
   Understand the type of data that you need. Be prepared to tell us about your research questions, the purpose of the project, funding, study population, variables requested, which traffic sectors data will come from, and your research methodology. If you plan to request individual-level data, you may need to receive approval from our data contributors. Be prepared to contact them and answer questions about your data request, including your questions and variables needed.

2. Complete a data request form.
   Once you have determined your data type, complete the appropriate form (see TRIP website for most current forms).

3. Submit your request to the TRIP.
   Email your data request to TRIP@ofm.wa.gov. Please allow up to a week for an initial response. The time it takes to review and fulfill a request depends on the complexity of the data.

Data Authorization Process

When the TRIP has received a data request, they begin the Data Authorization Process:

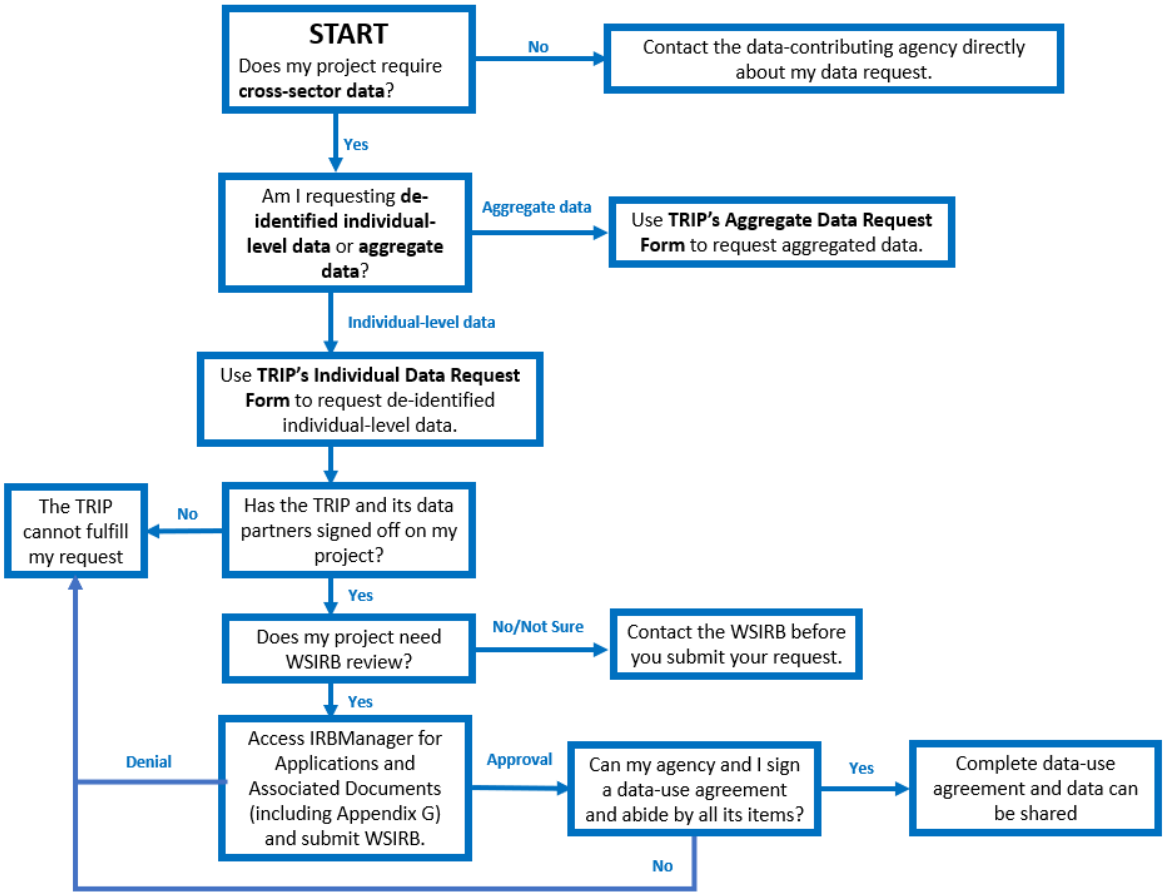
1. Data request received in the TRIP inbox.
   The data request form is saved and assigned the request a request or "R" number (ex. R5123).

2. Data request reviewed by the TRIP Staff Members
   Figure 3 illustrates the data approval process. The TRIP team reviews data requests to answer the following questions:
   a. Does the TRIP have jurisdiction to process the request?
   b. Is this request fulfillable? Is it feasible for the TRIP to fulfill with data currently available?
   c. Are the minimum data elements to answer the research questions being requested?
   d. Does the DSA with the data contributor clearly authorize this request/use of the data?
   e. Does the request need WSIRB approval?[2]
   f. Can the requestor meet TRIP data security standards?

[2] Per RCW 42.48, the WSIRB is the only governing entity to review request. All other IRBs must cede to the WSIRB. Review the WSIRB website to determine if request needs WSIRB approval.

3. If the project is approved to move forward, the TRIP will notify the data requestor if they need to contact any data contributors. Data requestor will work with OFM to complete Appendix G (State Agency Records Request) of the WSIRB application for AOC, DOT, DOL, and WSP data before submitting the WSIRB Application. If the data requestor is interested in DOH data, the data requestor will need to work with DOH to complete Appendix G before submitting WSIRB Application.

Figure 3: The TRIP Approval Process



Data Sharing Agreement (DSAs)

After an external request has been approved by data contributors and before it can be fulfilled, the TRIP must establish a data sharing agreement with the data requestor. The TRIP is supported by the OFM Information Technology contracts staff to guide this request. Each agreement with the data contributing agency is negotiated independently. There are several key components essential to ensuring the data is shared securely, and in compliance with relevant state regulations. This includes but is not limited to purpose and scope, data security and privacy protections, data ownership and rights, data retention and disposal, liability and indemnification, audit and monitoring.

The following process will be followed when entering a Data Sharing Agreement with another state agency or other stakeholder(s) to advance the interests of the TRIP. A sample TRIP DSA is attached in Appendix A: Sample DSA.

1. The TRIP will review the data request, including the benefits of entering into an agreement, the requirements of both parties, and the steps necessary to execute the agreement.
2. OFM drafts agreement using the appropriate DSA template. The OFM contract team drafts an agreement using the template and the data request form submitted by the researcher. The data request form typically includes information about the scope, timeline, research questions, and specifies the data elements that are being requested. It also details the cohort and years of data requested. All this information is included in the agreement.
3. OFM sends draft to data requestor for review and clarifies any missing information. If necessary, OFM seeks clarification on any items missing in the DSA not covered in the data request form and asks for the DSA administrator and privacy administrator of the requesting agency.
4. Requesting agency reviews and notifies OFM if they have concerns or if they are ready to sign. Once the requesting agency has reviewed and agrees with the terms of the DSA, the OFM Information Technology contracts staff sends them an electronic copy for signatures via DocuSign.
5. The data will be received in a manner agreed upon by both parties. OFM determines method for delivery of data. OFM can deliver data using a MFT account. Choosing the method of delivery informs what type of protections and requirements need to be applied in the data sharing agreement.
6. OFM will also require signed confidentiality and non-disclosure agreements for any individuals at the requesting agency that access the data through the analysis or review process.
7. OFM and the TRIP staff will integrate the data into the TRIP repository, scrubbing, cleaning, and otherwise preparing the data so that it can be used seamlessly in the TRIP research efforts.

Requirements for DSAs

Washington Technology Solutions (WaTech)'s Office of Privacy and Data Protection (OPDP) provides guidance and outlines requirements for state data sharing agreements. All OFM contracts are reviewed to ensure it meets state and federal requirements and best practices.

The following is an excerpt from the Data Sharing Agreement Implementation Guidance (December, 2021) created by the OPDP:

"Broad DSA requirements (in addition to requirements that may apply to specific agencies or specific types of information) exist for Washington state agencies in at least three places:

- RCW 39.34.240(1) states that "[i]f a public agency is requesting from another public agency category 3 or higher data . . . the requesting agency shall provide for a written agreement

between the agencies . . . .” Within chapter 39.34 RCW, a public agency means any agency, political subdivision, or unit of local government; any state agency; any United States agency; any federally recognized tribe; and any political subdivision of another state.

- OCIO Policy #141.10 states that “[w]hen sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law.” OCIO Policy #141.10 applies to executive branch agencies and agencies headed by separately elected officials.

Taken individually these requirements could conceivably be interpreted to create a patchwork of DSA mandates. But together they reinforce the best practice that an agency should typically enter DSAs when a person outside the agency receives or has access to confidential information. Entering into DSAs is also consistent with the Washington State Agency Privacy Principles. It is most obviously a core part of the due diligence principle, which requires exercising care when sharing information with third parties. DSAs also support the remaining principles by carrying forward the agency’s own obligations as a trusted steward of information and are one part of ensuring an agency understands all the places where its data is located.”

OCIO Data Categories

OCIO Policy 141.10 Securing Information Technology Assets, Standard 4.1 Data Classification requires that agencies "must classify data into categories based on the sensitivity of the data." Additionally, Agency data classifications must translate into or include 4 categories identified by the OCIO. Under 141.10, 4.2 Data Sharing, when sharing Category 3 or 4 data outside the agency, an agreement must be in place unless otherwise prescribed by law. The agreement must, among other things, include the categorization of the data.

The Division, in coordination with OFM Legal and Legislative Affairs' contracts unit, prepares Data Sharing Agreements and Data Use Agreements. Data Classification Agencies must classify data into categories based on the sensitivity of the data. Agency data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

(2) Category 2 – Sensitive Information
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

(3) Category 3 – Confidential Information
Confidential information is information that is specifically protected from either release or disclosure by law. This includes but is not limited to:

- Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
- Information about public employees as defined in RCW 42.56.250.
- Lists of individuals for commercial purposes as defined in RCW 42.56.070 (9).
- Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

(4) Category 4 – Confidential Information Requiring Special Handling
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

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

Appendix A: Sample DSA

DATA SHARING AGREEMENT BETWEEN
STATE OF WASHINGTON
OFFICE OF FINANCIAL MANAGEMENT
AND
RESEARCHER
For TRIP Data Shared Via File Transfer

This Data Sharing Agreement (DSA) is entered into by and between the **OFFICE OF FINANCIAL MANAGEMENT** (OFM) and (RESEARCHER) pursuant to the authority granted by Chapter 39.34 of the Revised Code of Washington, relevant federal statutes, and related regulations.

AGENCY PROVIDING DATA: OFFICE OF FINANCIAL MANAGEMENT
xxxxx

ORGANIZATION RECEIVING DATA: RESEARCHER
xxxxx

1. PURPOSE OF THE DSA

It is the purpose of this Agreement for OFM to provide information to the researcher to aid the success of the Traffic Records Integration Program ("TRIP"). The purpose of TRIP is to develop and maintain a database for public safety research to further the goals of the Vision Zero 2030 strategic plan adopted by Washington State.

The TRIP database will link data from several state agencies and will be leveraged to explore once inaccessible relationships in traffic safety data to save lives. TRIP will provide a platform for public and health safety research extending outside of OFM and WTSC. The data will be available through TRIP's data request process to ensure transparency as well as to maximize public safety research efforts.

The research conducted through TRIP will focus on xxxx.

This DSA documents operating procedures, roles and responsibilities, and appropriate data security constraints required for exchange of data between OFM and RESEARCHER.

All research projects must receive approval from the Washington State Institutional Review Board ("WSIRB"). The purpose of this research project is outlined in the application: xxx. Project must be approved by WSIRB prior to sharing of data. Any deviations from the project must be approved by TRIP and WSIRB.

1. DEFINITIONS

"**Agreement**" means this Data Sharing Agreement, including all documents attached or incorporated by reference.
"Confidential Information" means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information comprises both Category 3 and Category 4 Data as described herein, which includes, but is not limited to, personal information. For purposes of this DSA, Confidential Information means the same as "Data."

"Contract Administrator" means the individual designated to receive legal notices and to administer, amend, or terminate this DSA.
"Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
"OFM Data" means data provided by OFM, whether that data originated in OFM or in another entity.
"**Researcher**" means any party accessing Confidential Information pursuant to this DSA, and includes the entity's owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.
"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

2. PERIOD OF AGREEMENT

This Agreement shall begin on the date of the last signature and end on xxxx, unless terminated sooner or extended as provided herein.

3. DESCRIPTION OF DATA TO BE SHARED

It will include linked xxx variables to xxxx. OFM will only share data approved by the Washington State Institutional Review Board in application number xxxx.

4. DATA CLASSIFICATION

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer (OCIO) and included in OCIO Standard No. 141.10. The Data that is the subject of this DSA is classified as indicated below:

☐ **Category 1 – Public Information**
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

☐ **Category 2 – Sensitive Information**
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

☐ **Category 3 – Confidential Information**
Confidential information is information that is specifically protected from release or disclosure by law. It may include but is not limited to:

a. Personal Information about individuals, regardless of how that information is obtained.
b. Information concerning employee personnel records.
c. Information regarding IT infrastructure and security of computer and telecommunications systems.

☐ **Category 4 – Confidential Information Requiring Special Handling**
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

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

5. INTENDED USE OF DATA

RESEARCHER will describe xxxx. This research will answer the following questions: xxxx. Only work approved by the Washington State Institutional Review Board in application number xxx shall be performed with the data provided. Any deviation could result in immediate termination.

6. DATA ACCESS

RESEARCHER will provide the OFM agreement administrators and technical contacts the names and job titles of all its personnel who are given access to the data. RESEARCHER will notify the agreement administrators and technical contacts immediately whenever an authorized person is terminated or otherwise leaves, and whenever a user's duties change such that the user no longer requires access to perform work for this agreement. RESEARCHER will request written permission from OFM before outsourcing any work identified in this Agreement to a subcontractor.

7. DATA TRANSMISSION

The Data comes directly to the Researcher through a direct server connection via WaTech' s Secure File Transfer service (or the equivalent service offered by WaTech such as Managed File Transfer both hereinafter referred to as SFT) and is provided.

(x) one time annually on.

Secure File Transfer is a multi-protocol (Hypertext Transfer Protocol Secure [HTTPS], Secure File Transfer Protocol/Secure Shell [SFTP/SSH] and File Transfer Protocol [FTPS]) secure file transport to perform manual single file or automated high-volume file transfers with business partners located in the United States or Canada.

Researcher will retrieve the Data from the SFT server and download it to its secure server on its network for further processing. Data will be sent to Researcher by placing the interface file in the agency "out" directory on the SFT server. Researcher is responsible to retrieve the data within two weeks of the file being available in the SFT service. If the file is not downloaded with fourteen days, it will be deleted. Once downloaded, Researcher will secure the data and provide access to only those authorized individuals who need the data to perform their official duties.

8. DATA SECURITY

All data provided by OFM shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement. RESEARCHER agrees to store data on one or more of the following media and protect the data as described:

1) Workstation Hard disk drives. Data stored on local workstation hard disks. Access to the data shall be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such smart cards. If the workstation is located in an unsecured physical location the hard drive must be encrypted to protect OFM data in the event the device is stolen.

2) Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the data shall be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or

other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers shall be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Backup copies for DR purposes shall be encrypted if recorded to removable media.

3) Data Protection: The Researcher must protect and maintain all Confidential Information gained by reason of this DSA against unauthorized use, access, disclosure, modification or loss. This duty requires the Researcher to employ reasonable security measures, which include restricting access to the Confidential Information by allowing access only to staff that have an authorized business requirement to view the Confidential Information.

4) Data Security Standards: Researcher must comply with the Washington Office of the Chief Information Security Offices' Security Standard No. 141.10.

5) Data Disposition: Upon request or when no longer needed, Confidential Information/Data must be securely disposed pursuant to Exhibit B except as required to be maintained for compliance with the law or accounting purposes. Receiving Party will provide written certification of disposition upon request using Exhibit B Certification of Disposal.

6) Data storage on portable devices or media.
   a) OFM data shall not be stored by RESEARCHER on portable devices or media unless specifically authorized within this Agreement. If so authorized, the data shall be given the following protections:
      i. Encrypt the data with a key length of at least 128 bits
      ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.
      iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
      iv. Physically protect the portable device(s) and/or media by:
         - Keeping them in locked storage when not in use;
         - Using check-in/check-out procedures when they are shared; and
         - Taking frequent inventories.

   b) When being transported outside of a secure area, portable devices and media with confidential OFM data shall be under the physical control of RESEARCHER staff with authorization to access the data.
   c) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.
   d) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs, Blu-Rays), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

9. CONSTRAINTS ON USE OF DATA

1) The Data being shared is provided by the OFM. In some cases, the Data may represent Confidential Information of multiple disclosing parties.

2) This DSA does not constitute a release of the Data for the Researcher's discretionary use. Researcher must use the Data received or accessed under this DSA only to carry out the purpose and justification of this agreement as set out in section 1, Purpose and Authority for Data Sharing and for the research purpose set forth in Section 4 Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted.

3) Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

4) Researcher agrees that any Data provided under this Data Sharing Agreement cannot be used to create a contact list for commercial purposes.

10. DATA PRIVACY

1) Researcher may not make any ad hoc analyses or other uses of the Confidential Information. Data not specified within this DSA, without obtaining prior written agreement from OFM.

2) Neither Washington State nor OFM guarantee the accuracy or fitness for purpose of the data provided. Researcher acknowledges and accepts all risk and liability its use or misuse of information provided pursuant to this Agreement. To the extent, if any, that the data will be shared by the Researcher with entities other than OFM, the Researcher shall include the following statement:

> "The research presented here utilizes individual level data from Washington Office of Financial Management (OFM). TRIP works collaboratively with, policymakers and partners to provide trustworthy information and analysis. The views expressed here are those of the author(s) and do not necessarily represent those of the OFM or other data contributors. Any errors are attributable to the author(s)."

3) Data provided by OFM under this Agreement shall not be linked with other data or data sets in any way that may disclose the identity of individuals or employers; the data in any data set shall be used for statistical purposes only. Using Confidential Information /Data to identify specific individuals may be cause for immediate termination of this Agreement. Further, at OFM's sole discretion, other data sharing agreements with the Researcher may also be subject to termination and OFM may decline requests for data sharing agreements with the Researcher in the future. If the identity is discovered inadvertently, Researcher will not use this information and will immediately inform OFM in writing of any such discovery.

4) Researcher must provide draft report(s) to OFM and data contributors at least sixty (60) working days prior to any public release of reports to verify proper disclosure avoidance techniques have been used and communicate with OFM or data contributors when questions arise regarding data provided.

5) OFM shall have the right, at any time, to monitor, audit and review activities and methods in Recipient's implementation of the Agreement in order to assure compliance therewith, within the limits of Recipient's technical capabilities. In addition, and in accordance with federal employment data law and data best practices, OFM, in its sole discretion, may require at Recipients expense, an inspection of Recipient to assure that the requirements of the state's law and data sharing agreement are being met. A list of Washington State approved auditing services companies is provided through the Department of Enterprise Services website:

https://fortress.wa.gov/es/apps/ContractSearch/ContractSummary.aspx?c=05913. You may choose one from the list or send a letter requesting a specific company that may only be used with the approval from OFM. Audits must be accomplished within the first year that the data was transferred, and every three years until termination of the Agreement, and carrying through to the destruction of data.

6) Researcher will provide an attestation that the Data will not be used for supplemental purposes and will not be shared with anyone (including publishers such as journals).

7) To the extent that any data included Toxicology Reports (WSP-TOX) as classified under RCW 46.52.065, Researcher agrees to adhere to all requirements stated in Chapter 46.52. The WSP-TOX data has been classified confidential, a higher classification than the crash data the information will be linked to. The classification of confidential will not change once the information is linked to the crash data.

8) Aggregate Driver and Vehicle Permissible use is for any governmental agency including any court or law enforcement agency, or any private person or entity acting on behalf of a federal, state, or local agency, or Canada in carrying out its functions: but nothing in this section is construed to allow actions prohibited under RCW 43.17.425.

Data Segregation

1) OFM data shall be segregated or otherwise distinguishable from non-OFM data. This is to ensure that when no longer needed by the RESEARCHER, all OFM data can be identified for return or destruction. It also aids in determining whether OFM data has or may have been compromised in the event of a security breach.
    a. OFM data shall be kept on media (e.g., hard disk, optical disc, tape, etc.) which shall contain no non-OFM data. Or,
    b. OFM data shall be stored in a logical container on electronic media, such as a partition or folder dedicated to OFM data. Or,
    c. OFM data shall be stored in a database, which will contain no non-OFM data. Or,
    d. OFM data shall be stored within a database and will be distinguishable from non-OFM data by the value of a specific field or fields within database records. Or,

2) When it is not feasible or practical to segregate OFM data from non-OFM data, then both the OFM data and the non-OFM data with which it is commingled shall be protected as described in this Agreement.

11. DATA CONFIDENTIALITY

RESEARCHER acknowledges the personal or confidential nature of the information and agrees that their staff and contractors with access shall comply with all laws, regulations, and policies that apply to protection of the confidentiality of the data. If data provided under this Agreement is to be shared with a subcontractor, the contract with the subcontractor shall include all of the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement.

a. Non-Disclosure of Data

    1) Individuals shall access data gained by reason of this Agreement only for the purpose of this Agreement. Each individual (staff and their contractors) with data access shall read and sign Exhibit A, Statement of Confidentiality and Non-Disclosure, prior to access to

the data. Copies of the signed forms shall be sent to the OFM Agreement Administrator identified on Page 1 of this Agreement, who will distribute them to the other traffic agencies as appropriate.

2) OFM may at its discretion disqualify at any time any person authorized access to confidential information by or pursuant to this Agreement. Notice of disqualification shall be in writing and shall terminate a disqualified person's access to any information provided by OFM pursuant to this Agreement immediately upon delivery of notice to RESEARCHER. Disqualification of one or more persons by OFM does not affect other persons authorized by or pursuant to this Agreement.

b. Penalties for Unauthorized Disclosure of Information
In the event RESEARCHER fails to comply with any terms of this Agreement, OFM shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

12. USE OF DATA

a. Data provided by OFM shall remain the property of OFM and shall be returned to OFM or destroyed when the work for which the information was required has been completed.

b. Data may only be used consistent with the WSIRB approved application and consistent with the restrictions and regulations of the WSIRB, located at: https://www.dshs.wa.gov/ffa/human-research-review-section.

c. This Agreement does not constitute a release of the data for RESEARCHER's discretionary use but may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of OFM. RESEARCHER shall not disclose, transfer, or sell any such information to any party, except as provided by law. RESEARCHER shall maintain the confidentiality of all Personally Identifiable Information and other information gained by reason of this Agreement.

d. RESEARCHER is not authorized to update or change any OFM data, and any updates or changes shall be cause for immediate termination of this Agreement.

e. Neither Washington State nor OFM guarantees the accuracy of the data provided. All risk and liabilities of use and misuse of information provided pursuant to this Agreement are understood and assumed by RESEARCHER.

f. Data provided by OFM cannot be linked with other data or data sets as a way to determine the identity of individuals or employers; the data in any data set shall be used for statistical purposes only. Using OFM data to identify individuals shall be cause for immediate termination of this Agreement and may prevent data sharing agreements with the organization in the future. If the identity of any individual is discovered inadvertently, RESEARCHER shall not use this information and shall advise OFM of any such discovery.

g. Data provided by OFM cannot be re-disclosed or duplicated unless specifically authorized in this Agreement.

h. RESEARCHER shall include the following excerpts with any public release using OFM data:

"The research presented here utilizes individual level data from Washington Office of Financial Management (OFM). TRIP works collaboratively with, policymakers and partners to provide trustworthy information and analysis. The views expressed here are those of the author(s) and do not necessarily represent those of the OFM or other data contributors. Any errors are attributable to the author(s)."

i. RESEARCHER shall provide draft report(s) to OFM and data contributors at least two months prior to any public release of reports and communicate with OFM or data contributors when questions arise regarding data provided.

j. The requirements in this section shall survive the termination or expiration of this agreement or any subsequent agreement intended to supersede this DSA.

13. DATA SHARED WITH SUBCONTRACTORS

If Data access is to be provided to a Subcontractor under this DSA, the Researcher must include all of the Data constraints, conditions and requirements set forth in this DSA in any such Subcontract, or verify that a substantially equivalent term is included. In no event will the existence of the Subcontract operate to release or reduce the liability of the Researcher for any breach in the performance of the Researcher's responsibilities.

14. DATA BREACH NOTIFICATION

The Breach of Data shared under this DSA must be reported to the appropriate Privacy Officer within one (1) business day of discovery. The Privacy Officer for each of the Parties is listed below. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by applicable law or reasonably requested in order to meet its regulatory obligations.

- OFM Privacy Officer- ofmmi@ofm.wa.gov
- Receiving Party Contact-

15. DISPOSITION OF DATA

Upon request or when no longer needed, Confidential Information/Data must be securely disposed pursuant to Exhibit B except as required to be maintained for compliance with the law or accounting purposes. Researcher will provide written certification of disposition upon request using Exhibit B Certification of Disposal

16. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

RESEARCHER agrees that OFM shall have the right, at any time, to monitor, audit and review activities and methods in implementing the Agreement in order to assure compliance therewith, within the limits of RESEARCHER's technical capabilities.

Both parties hereto shall retain all records, books, or documents related to this Agreement for six years, except data destroyed in Section 9. The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this period.

17. PUBLIC RECORDS

RESEARCHER acknowledges that OFM is subject to the Public Records Act (Chapter 42.56 RCW). This DSA will be a "public record" as defined in Chapter 42.56 RCW. Any documents submitted to OFM by may also be construed as "public records" and therefore subject to public disclosure. If the OFM receives a public records request under Chapter 42.56 RCW for any records

containing Data subject to this DSA that was provided by a Researcher, OFM will notify the Researcher of the request within 3 business days before disclosing any records.

18. ASSIGNMENT

The RESEARCHER will not assign rights or obligations derived from this DSA to a third party.

19. INDEMNIFICATION

Each party to this Agreement shall be responsible for any and all acts and omissions of its own staff, employees, officers, agents and independent contractors. Each party shall furthermore defend and hold harmless the other party from any and all claims, damages, and liability of any kind arising from any act or omission of its own staff, employees, officers, agents, and independent contractors.

20. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT

With mutual consent, OFM and RESEARCHER may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff.

21. TERMINATION

a. <u>For Convenience</u>
Either party may terminate this Agreement with thirty (30) days' written notice to the other party's Agreement Administrator named herein. In case of termination, any and all information provided by OFM pursuant to this agreement shall either be immediately returned to OFM or immediately destroyed. Written notification of destruction to OFM is required.

b. <u>For Cause</u>
OFM may terminate this Agreement at any time prior to the date of completion if and when it is determined that RESEARCHER has failed to comply with the conditions of this Agreement. OFM shall promptly notify RESEARCHER in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the data provided by OFM shall be returned to OFM or destroyed on or before the date of termination. Written notification of destruction to OFM is required.

22. GOVERNING LAW

This Agreement shall be construed under the laws of the State of Washington. Venue shall be proper in Superior Court in Thurston County, Washington.

23. SEVERABILITY

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court; that invalidity shall not affect the other provisions of this Agreement and the invalid provision shall be considered modified to conform to the existing law.

24. SIGNATURES

The signatures below indicate agreement between the parties.

Exhibit A

STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE
between the
State of Washington
OFFICE OF FINANCIAL MANAGEMENT
and the
RESEARCHER

As an employee of RESEARCHER, I have access to information provided by the State of Washington, Office of Financial Management (OFM). This information is confidential, and I understand that I am responsible for maintaining this confidentiality. I understand that the information may be used solely for the purposes of work under DSA No. xxx.

- I have been informed and understand that all information related to this DSA is confidential and may not be disclosed to unauthorized persons. I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any information contained in this system.
- I also understand that I am not to access or use this information for my own personal information but only to the extent necessary and for the purpose of performing my assigned duties as an employee of RESEARCHER under this Agreement. I understand that a breach of this confidentiality will be grounds for disciplinary action which may also include termination of my employment and other legal action.
- I agree to abide by all federal and state laws and regulations regarding confidentiality and disclosure of the information related to this DSA.

Employee
I have read and understand the above
Notice of Nondisclosure of information

Signature _____

Printed Name _____

Organization _____

Job Title _____

E-mail address _____

Date _____

Supervisor
The employee has bene informed of their obligations including any limitations, use or publishing of confidential data.

_____

_____

_____

_____

_____

_____

Please return signed forms to OFM, PO Box 43124, Olympia, WA 98504-3124

Exhibit B

Certificate of Document/Data Destruction

The purpose of this document is to confirm the destruction or exacted data from the Office of Financial Management as per the terms and conditions of the Data Sharing Agreement with you. A signed Certificate of Destruction and confirmation of receipt by the OFM DSA Administrator Data constitutes acknowledgement that the data was appropriately destroyed.

Submit your completed form to the names DSA Administrator in the Umbrella Data Sharing Agreement.

Your Name	
Your contact information	
Data Sharing Agreement Entity Name	
Data Sharing Agreement Number	

Are both the DSA and an Addendum ending? Yes/No
If only an Addendum is ending- what is DSA Addendum Name and Number:
_____

Original Media

If data was provided to you on original media (e.g. CD, DVD, floppy disk, server access) you MUST be destroyed using the methods as described in Schedule A. Please complete the following section as applicable.

Data Delivery Date	Data Contents	Data Delivery Type	Destruction Method	Destruction Date

If no original media was provided, initial here _____.

Locally Stored Copies of Data and Derived Information

All electronic copies of Data in ALL devices (e.g., desktops, laptops, hard drives) throughout the entire duration of the agreement, including devices used by all team members with access to the data MUST be destroyed using the methods described in Schedule A. Please complete the following section as applicable. Please from a log output from the wiping software or erasure program used.

Data Storage location	Wiping Software Used	Date Wiping Software Used

If you did not use a wiping software, please explain in detail your data destruction methods:

DECLARATION OF DESTRUCTION

I declare that the methods described above for Data destruction are for ALL THE DEVICES (including CD-ROMS, floppy discs, flash drives, etc. used for backing up files) of all team members with access to the data for the duration of the whole project. I further declare that all stored data has been deleted and erased from existing systems, either owned by or provided to me.

I understand that this document is legally binding, and that falsifying this information would constitute a breach of my Data Sharing Agreement with OFM.

I, name, declare that the information provided in this document is accurate, complete, and correct. I declare that I have destroyed all original media, copies of the data, derived information and any related backups with the data as per the terms of the Data Sharing Agreement with OFM.
Name_____
Date_____

Schedule A Resources for Data Destruction

Maintain secure control and custody of media to be disposed

- Media to be disposed must stay within the control of the agency from the time it is collected to the time it is sanitized. Pick-up/Transit – Storage media to be disposed should be collected by, and in the constant possession of dedicated, trusted personnel
- Media should be maintained in a secure, locked area until it can be sanitized

Render *all* data on the media unusable.

When files are deleted from a computer, emptied from the Recycle Bin or even by reformatting, if it is not overwritten it can be easily recovered using commonly available tools.

- Don't delete the data – destroy it

- All data should be rendered unusable using special software designed for this purpose (See examples at bottom of page)
- Meets the requirements of Section 8.3 of the OCIO IT Security Standards

Physical destruction is an option.

- Agencies may physically destroy the media itself rather than sanitize the media
- This typically takes the form of shredding or pulverization, ensuring the media can never be used again. Any media that cannot be sanitized through the use of software tools must be physically destroyed.

Private companies are available to perform this service, and agencies must be sure that they can maintain control of the media from the time it leaves the agency until the time it is actually destroyed. When pursuing this option, agencies should consider those companies that dispose or recycle these materials in an environmentally responsible way.

Keep Detailed Records

Agencies should maintain records that document all media disposal activities, as this can provide agencies with the means of confirming that specific media was disposed of properly if it is later called into question.

Records for disposed media should include:

- Information about the media (type, serial number, other unique identifiers) The date the media was sanitized
- The person performing the activity
- The method used to render all data unusable (e.g. software tool used or physical destruction of the media)
- The signature of the person responsible for ensuring that all data on the storage media has been rendered unusable.

Free Data Erasure Software

Free software utilities that can be used to meet OCIO IT Security Standards data and media disposal requirements:

Active@KillDisk - http://www.killdisk.com [1]

- Data Sanitization Methods: DoD 5220.22-M, GOST p50739-95, NSA 130-2, Schneier, Gutmann, 21-23 NIST 800- 88, Random Data, Write Zero

Eraser Portable - http://portableapps.com/apps/security/eraser-portable [2]

- Data Sanitization Methods: DoD 5220.22-M, AFSSI-5020, AR 380-19, RCMP TSSIT OPS-II, HMG IS5, VSITR,
  GOST R 50739-95, Gutmann, Schneier, Random Data

Microsoft's SDelete - http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx [3]

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data

Freeraser - http://download.cnet.com/Freeraser/3000-2144_4-10909403.html [4]

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data