<insert organization logo or award recipient letterhead>

Data Management Plan
for the Bureau of Justice Statistics (BJS)

Award Recipient Name:
BJS Project Name:
Award #:
Award period:
Date:

DOCUMENT CHANGE/REVISION HISTORY					
Section/ page #	**Summary of changes**	**Author**	**Date**	**Version**	**Date of BJS approval**

Data Management Plan

Table of Contents

Overview

The Bureau of Justice Statistics (BJS) requires, as a condition of funding, BJS award recipients that collect or maintain data under BJS's authority to develop and maintain a current BJS-approved data management plan (DMP). The DMP summarizes the procedures and controls that will be used to handle, process, store, disseminate, and dispose of the data collected or maintained in conjunction with the BJS-funded activities.

For projects including the collection or maintenance of information identifiable to a private person, the DMP will include all applicable provisions required of a Privacy Certificate (28 C.F.R. § 22.23(b)) to describe the specific controls in place to protect data security and confidentiality.

The award recipient should collaborate with the BJS Project Manager to develop the data management plan. **The DMP should be submitted to BJS no later than 60 days after the award start date and must be approved by BJS before data collection activities begin**

The DMP is a living document that will be updated as needed throughout the award period. BJS must approve modifications to the plan (changes in the technologies that will be used, vendors, data transfer or storage methods, scope of data collection, etc.) *in writing* before they are implemented. Modifications may also require notice to and approval by an Institutional Review Board (IRB), in addition to any required internal approvals from the award recipient agency.

This template provides a framework that BJS award recipients may use to determine what information to report and how to organize it. An award recipient may use its preferred format to report the information. BJS encourages its award recipients to provide additional information beyond the examples provided to describe its data handling, processing, protection, and storage activities.

Project and Deliverable Information

Basic Project Information	
BJS program/project name	
Award number	
Award recipient name	
Award period	
Award recipient POC for data management plan and contact information	
BJS program manager	
IRB number and expiration date, if applicable	

Please list the key deliverables associated with data collection, dissemination, and disposition tasks associated with this DMP.

Deliverables	
Deliverables (*examples provided*)	**Date sent to BJS**
• *Final data management plan approved*	
• *Paperwork Reduction Act clearance materials*	
• *Draft statistical tables*	
• *Draft report*	
• *Archive file*	
• *Certificate(s) of Data Destruction*	

Data Collection and Analysis Procedures

This section describes basic information about how and what types of data will be collected or maintained in conjunction with the BJS-funded activities. It also describes the tools and procedures that will be used to handle and process the information.

Examples of what information to provide for the following key categories:

Data collection/acquisition

- *Data source(s), e.g., administrative records from jail facilities, inmate interviews, surveys, etc.*
- *File categories, e.g., personally identifiable information (PII) versus public data*
- *Specific PII elements that will be collected (e.g., name, SSN, other identifying number)*
- *File format(s) that will be used*
- *File sizes (estimate)*
- *Type of physical media used, e.g., paper surveys*
- *Software tools, applications, and/or programs that will be used to collect the data, e.g., webform application*

Data processing

- *Software tools that will be used to process the data, e.g., STATA, SAS, WinZip, etc. for:*
    - *Primary data that will be acquired or collected from BJS or a data provider*
    - *Supplemental data that will be used to process the data, e.g., public-use files, metadata, or data file from another federal agency (if applicable)*

These examples do not represent an exhaustive list of information that an award recipient can report in this section. Additional details should be provided as determined by the award recipient or as requested by BJS.

Data Security and Confidentiality Procedures

This section describes how the data collected or maintained in conjunction with the BJS-funded project will be stored and safeguarded.

For projects that include information identifiable to a private person, this section should describe all applicable provisions required of a Privacy Certificate (28 C.F.R. § 22.23(b)) to describe the specific technical, physical, and administrative controls in place to protect data security and confidentiality.

Examples of what information to provide for the following key categories:

Data Storage

- *Computing environment*
- *Storage areas for physical media*
- *File path locations (where and in what folders will the data be stored in the system)*
- *Sensitivity categorizations applied to the information*
- *Backup procedures*
- *For systems that are used to store, process, and analyze PII or other sensitive information, describe:*
    - *If the system is compliant with Federal Information System Modernization Act (FISMA) requirement? At what level (e.g., moderate or high)?*
    - *If the system is compliant with Federal Information Processing Standards (FIPS) 140-2*
    - *If National Institute of Standards and Technology (NIST) standards are followed to classify the risk sensitivity and categorize the information*
    - *Other federal standards the system is compliant with*
    - *What authentication controls are employed*
    - *Procedures to ensure BJS PII is not comingled with other non-BJS or non-project data*

Access

- *Specific access controls and technologies that will be used to restrict, log, and track access to PII, e.g., including role and group permissions*
- *Remote access procedures, e.g., use of Virtual Private Network (VPN)*
- *External access procedures, e.g., VPN and secure file transfer portal*
- *Firewalls and other perimeter protection controls*
- *Security controls, including anti-spam, anti-malware, and anti-intrusion tools*

Information transfer exchanges

- *Methods to transport information to and from BJS*
    - *DOJ JEFS must be used when transferring PII or other sensitive information to and from BJS unless BJS approves another secure exchange*

- *Methods to transport information from a data provider to the study team, and/or the study team to another authorized partner (e.g., subcontractor)*

- *For exchanges that will be used to transfer information containing PII or other sensitive information, including data files and work products, to and from internal staff, data providers, or external partners (e.g., authorized subcontractors), describe:*

    - *Application that will be used to transfer data, if different than JEFS*
    - *Procedures to ensure data are encrypted in transit and while at-rest*
    - *Methods to securely transport physical media containing PII*

These examples do not represent an exhaustive list of information that an award recipient can report in this section. Additional details should be provided as determined by the award recipient or as requested by BJS.

Audit and Accountability

This section describes the procedures in place to ensure system integrity and compliance with data security, confidentiality, and privacy standards.

For projects that do not include PII or other sensitive information, this section should describe how the integrity of the system is maintained and monitored.

Examples of what information to describe include:

- *Procedures to ensure compliance with security and privacy standards and requirements*
- *Logging capabilities to ensure that only authorized users access restricted folders*
- *Reporting procedures to investigate suspicious or anomalous activity or suspected violations*

These examples do not represent an exhaustive list of information that an award recipient can report in this section. Additional details should be provided as determined by the award recipient or as requested by BJS.

Data Use Agreements or Memorandum of Understanding

This section lists relevant data use agreements (DUA) or Memoranda of Understanding (MOU) that are executed during the award period and describes any special requirements the award recipient is required to fulfill, beyond the responsibilities described in 28 CFR Part 22.

Award recipient may denote N/A if no agreements will be executed in conjunction with the award.

Name of DUA or MOU (examples provided)	Data provider	Date executed (signed)	Expiration date	Special requirements (examples provided)	Procedure(s) to ensure compliance	Date of completion
Data use agreement between Orange County Jail and BJS	*Orange County Jail*	*April 2, 2022*	*April 1, 2025*	*Sign nondisclosure agreement*	*All project staff will sign an NDA and send them to the data provider; will retain copies as an auditable requirement*	*TBD*
MOU with the FBI	*FBI*	*April 4, 2022*	*April 3, 2027*	*Complete FBI-required data security training*	*Project staff will complete training and submit certificate of training to the BJS Program Manager*	*TBD*

Security Incident Response

This section describes the procedures that project staff will follow to report a real or suspected security incident involving PII that is collected or maintained in conjunction with the BJS-funded project. BJS will provide a copy of its guidance on security breach or incident response.

Examples of what information to describe include:

- *Procedures to identify and report a real or suspected security incident involving PII or other sensitive information that is collected or maintained under the award*
- *Types of security incidents that will be reported (e.g., transferring sensitive data using a method not approved in this data management plan)*
- *Affirmation that BJS Security Incident Reporting Procedures will be followed (BJS will provide a copy of the procedures)*

Data Disposition

This section describes the procedures that will be followed to comply with BJS's data disposition requirements, as described in the relevant award special condition.

Examples of what information to describe include:

- *Procedures to ensure compliance with BJS requirement to return and destroy all PII and other nonpublic information at the end of the award period*
    - *Affirmation that pathways and file locations where PII and nonpublic information will be stored will be logged to ensure all required information is returned to BJS and destroyed*
    - *Acknowledgement that data disposition activities will be reported in semi-annual and final performance reports*
    - *Affirmation that no PII or nonpublic information will be destroyed without BJS's written approval*
- *Specific disposition methods and techniques that will be used*
- *Process to delete PII and nonpublic data from backup files and servers*
- *Acknowledgment that a signed data destruction certificate will be provided to BJS*

Staff training

This section describes the relevant trainings project staff are required to complete as part of their responsibilities related to handling data collected or maintained in conjunction with the BJS-funded project.

Examples of what information to report include:

- *List of trainings related to data security, privacy, and/or confidentiality*
- *Brief description of training content*
- *Training completion dates*

Summary of Lifecycle and Pathways

This section summarizes relevant information to describe what, how, and where electronic and physical records will be stored, transferred, and disposed of. It also summarizes the physical controls that will be applied to safeguard the information collected or maintained in conjunction with the BJS-funded project. *The charts serve as examples; the award recipient may report relevant information in whatever format they choose.*

Pathway of Electronic Records							
Information source (e.g., BJS or data provider)	**Type of information**	**Recipient**	**Transfer method**	**Storage system**	**Data destruction method**	**Data destruction date**	**File path location**
BJS	*Offender records*	*<award recipient>*	☐ *JEFS* ☐ *Other: describe*	☐ *Secure server* ☐ *Network project folder* ☐ *Non-network computer*	☐ *File shredder (7 pass)* ☐ *Secure delete (SDelete 7 pass)* ☐ *Other: describe*	*Award expiration date*	<insert>
<data provider>	*Inmate survey responses*	*<award recipient>*	☐ *Secure webform* ☐ *Other: describe*	☐ *Secure server* ☐ *Network project folder* ☐ *Non-network computer*	☐ *File shredder (7 pass)* ☐ *Secure delete (SDelete 7 pass)* ☐ *Other: describe*	*Award expiration date*	<insert>

Pathway of Physical Records							
Source	**Type of information**	**Recipient**	**Transfer method**		**Storage site**	**Data destruction method**	**Data destruction date**
BJS	*Inmate interviews*	*<award recipient>*	☐ *Paper* ☐ *Encrypted CD/DVD* ☐ *Tape* ☐ *Encrypted thumb drive* ☐ *Encrypted hard drive*	☐ *USPS (Registered)* ☐ *UPS* ☐ *FedEx* ☐ *Hand-delivered: by whom* ☐ *Fax*	☐ *Locked cabinets or storage room* ☐ *Alternate secure site: describe*	☐ *Shredding* ☐ *Degaussing* ☐ *Other: describe*	

Physical Access Controls			
Organization	**Building access**	**Room access**	**Media access**
<data provider staff>	☐ Key card ☐ Biometric imprint ☐ Other method: describe	☐ Key card ☐ Biometric imprint ☐ Other method: describe	☐ Key card ☐ Biometric imprint ☐ Other method: describe
<subcontractors or consultants>	☐ Key card ☐ Biometric imprint ☐ Other method: describe	☐ Key card ☐ Biometric imprint ☐ Other method: describe	☐ Key card ☐ Biometric imprint ☐ Other method: describe

Additional information

The section includes any additional information requested by BJS.

Examples of information that may be requested (at the discretion of the BJS Program Manager):

- *Data dictionaries*
- *List of specific variables that will be collected or maintained*

Appendices

This section includes supplemental information, as provided by the award recipient or as requested by BJS.