DSS-J POLICY MANUAL

Article I. Definitions and Governance Structure

Section 1.01 Definitions

The following terms have the meanings specified below. See DSS-J Intergovernmental Agreement between the County and each Member Agency for additional definitions of terms not explicitly defined in this manual.

(a) Aggregate Data: Individual Data records that have been combined into summary level statistics. In most cases, aggregate Data does not include the underlying individual Data records and is de-identified.

(b) Criminal Justice Information (CJI) Data: Refers to the Data contributed by a Source Agency to DSS-J from a criminal justice information system (CJIS) that is regulated under 28 CFR Part 20, subparts B or C, and necessary for that Criminal Justice Agency to perform its mission related to the Administration of Criminal Justice, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information (PII), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

i. See **Appendix C** for current list of fields in DSS-J that are CJI Data.

(c) Criminal Justice Agency (CJA): Means: (1) courts; and (2) a governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included. 28 CFR § 20.3(g).

(d) Data: Refers to any information contributed by a Member Agency, regardless of format, to the DSS-J, including, without limitation, CJI.

(e) Data Governance: The exercise of decision-making and authority for Data-related matters that results in improved quality, easier access, and managed and auditable security over Data. Data governance sets the direction for quality assurance and quality control and then monitors the success of those efforts, and may include:

(i) Identification of Data Stewards for all DSS-J agencies (Source and Member).

(ii) The creation of an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of Data.

(iii) A set of roles that specifies who can take what actions with what Data, and when, under what circumstances, using what methods.

(iv) Definitions of processes, roles, standards and metrics that ensure the effective and efficient use of Data in enabling DSS-J users to achieve their goals.

(v) Developing controls to manage the risk of Data quality issues, Data naming and business rules conflicts, Data security issues, and service level problems

(f) Data Stewards (designated Source Agency analyst): Each Source Agency is responsible for designating one or more individual(s) to serve as that Source Agency's Data Steward(s). The Data Steward(s) may be a Source Agency's analyst and/or a DSS-J Identified User. This person will be the primary point-of-contact for Data quality assurance and quality control work.

(g) Data Trustee: Each Source Agency is responsible for designating one executive-level individual to serve as the Source Agency's Data Trustee. The Data Trustee is an executive-level individual who is responsible for, and assumes administrative control over, granting access to a Source Agency's Data.

(h) DSS-J: Decision Support System – Justice is a public safety data warehouse that integrates public safety Data from Member Agencies. DSS-J enables Identified Users to query Member Agency Data, track events such as criminal incidents, arrests, case dispositions and sentencing across data systems, and respond to requests for research regarding operational and policy issues affecting the public safety system.

(i) Identified User: Is any person authorized by a Criminal Justice Agency that has signed an agreement with County substantially similar in the form attached IGA, to access and use DSS-J that: (i) is an Authorized User; (ii) has acknowledged they will access Data including, without limitation, CJI only for an Authorized Use; and (iii) has agreed in writing to follow the terms of this Policy manual and the applicable IGA.

(j) Intergovernmental Agreement (IGA): Defined in Section 2.01(a).

(k) Host Agencies: Collectively, Multnomah County ("County"), acting through its Local Public Safety Coordinating Council (LPSCC), the Multnomah County Sheriff's Office (MCSO), the Multnomah County District Attorney's Office (MCDA), and the Department of Community Justice (DCJ).

(l) Member Agency: The Host Agencies and any other Criminal Justice Agency who has agreed to and signed the IGA with County and agreed to comply with this Policy Manual.

(m) Non-Member Agency or Agencies: A CJA that has not entered into an IGA for access and use of the DSS-J.

(n) Personally Identifiable Information (PII): PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

ii. Examples include: name, address, phone number, email, social security number, passport number, driver's license number, vehicle plate, fingerprint data, credit card numbers, date of birth, birthplace.

iii. See **Appendix C** for current list of fields in DSS-J that are PII.

(o) Policy Manual: The DSS-J Policy Manual (this document) defines and describes the roles, responsibilities and governing structure related to DSS-J Data governance as well as rules for Data use and user responsibilities. The Policy Manual also provides a description of the DSS-J and defines rules around Data security and Data sharing.

(p) Quality Assurance (QA): The goal of QA is to mitigate defects in future Data products. QA identifies and ensures the business rules around how Source Data is transferred and uploaded to DSS-J, and transformed for analytical use.

(q) Quality Control (QC): The goal of QC is to identify defects within a product before it is released. It is the practice of making sure Data are accurate and usable for the intended purpose.

(r) Security Policy: Refers to version 5.9 of the Criminal Justice Information Services Security

Policy, CJISD-ITS-DOC-08140-5.9, published by the Federal Bureau of Investigation.

(s) Source Agency: A Member Agency that contributes Source Data to DSS-J.

(t) Source Data: A Member Agency's Data contributed by that Member Agency to the DSS-J.

Section 1.02 Roles and Responsibilities

(a) DSS-J Policy Team (see Appendix A):

Members include policy representatives from LPSCC, all Source Agencies, and other criminal justice stakeholders as more particularly set forth in **Appendix A**.

(i) Members may be those charged with the authority to sign Intergovernmental Agreements or Data Sharing Agreements on behalf of their agency.

(ii) Responsibilities of DSSJ- Policy Team:

a. Identify and define business problems.

b. Develop research questions.

c. Review and approve requests for DSS-J Data made by Non-Member Agencies pursuant to the procedures outlined below in this Section 1.02(a)(iii).

d. Consider requests for DSS-J access made by Non-Member Agencies and decide the appropriate course of action for formal approval of new DSS-J Member Agencies.

e. Act as executive sponsors, as required per project.

f. Define processes around access and use of DSS-J consistent with this Policy Manual.

g. Define/confirm priorities.

h. Acknowledge DSS-J project milestones.

i. Work with appropriate Member Agencies to develop MOUs/IGAs, as needed.

(iii) Criteria for approval by the DSS-J Policy Team: Subject to the approval requirements of other sections of this Policy Manual and except for requests by Non-Member Agencies for access to DSS-J or use of Data, the DSS-J Policy Team shall make decisions based on majority approval (at 50%) of all Policy Team members. With respect to requests by Non-Member Agencies for access to DSS-J or use of Data, the DSS-J Policy Team must approve such requests by unanimous consent.

(b) DSS-J Operations Team (see Appendix B):

Members include representatives from LPSCC, all Source Agencies, and DSS-J IT.

(i) Members may be in management positions in IT or research units at the agency-level.

(ii) Responsibilities of DSS-J Operations:

a. Governance and operational oversight as outlined in this Policy Manual.

b. Review and approve DSS-J research projects made by Identified Users representing Member Agencies requesting use of DSS-J Data (see **Appendix B**).

c. Receive and review outside agency requests for DSS-J Data.

d. Provide recommendations to the Policy Team.

e. Establish DSS-J business processes and procedures that comply with this Policy Manual.

f. Facilitate vertical communication across DSS-J Member Agencies.

g. Plan and facilitate Policy Team meeting agendas, as needed and appropriate.

h. Brief Policy Team Members on issues, as needed.

i. Receive and prioritize project requests and communicate priorities back to the appropriate DSS-J body.

j. Regularly review Identified User access.

(iii) Criteria for approval by the DSS-J Operations Team: Subject to the approval requirements of other sections of this Policy Manual and except for requests by Non-Member Agencies for use of Data, the DSS-J Operations Team shall make decisions based on majority approval (at 50%) of all Policy Team members. With respect to requests by Non-Member Agencies for use of Data, the DSS-J Operations Team must approve such requests by unanimous consent.

(c) DSS-J User Group (see Appendix B)

(i) Participation is open to all Identified Users and DSS-J IT.

(ii) Responsibilities of DSS-J User Group:

a. Identify DSS-J bugs.

Receive and prioritize low-level DSS-J requests that have been reviews and approved by the Operations Team (e.g., small projects).

b. IRB considerations for research involving human subjects that potentially includes Data from DSS-J and comply with that processes as needed.

c. Maintain training documents, DSS-J schema, and Data dictionaries.

d. Conduct Data analysis and complete Data-related projects, as prioritized. See Articles *3.02 through 3.06 and Articles* 4.04 through 4.06 for rules related to Data access, use, and analysis.

(d) DSS-J Work Groups

(i) When necessary, DSS-J work groups may be formed to address a specific topic or project on an ad hoc basis (e.g., bringing in new Data, building new datasets using Data ("Datasets"), or creating standards for use of particular Data).

(ii) Work groups operate under the authority of standing DSS-J groups, including User Group, Operations Team, or Policy Team.

(e) DSS-J IT

(i) Responsibilities of DSSJ-IT:

a. Manage critical DSS-J databases.

b. Work with Source Agencies to ensure Data is accurately reflected in DSS-J.

c. Participate in all levels of DSS-J governance, including the Policy Team, Operations Team, and User Groups.

d. Respond to requests from Identified Users for maintenance or building efforts within DSS-J.

e. Acknowledge receipt of each request from a Source Agency to remove sealed or expunged cases from the DSS-J warehouse.

(f) Source Agency

(*i*) DSS-J maintenance responsibilities of the Source Agency:

a. Facilitate assurance that the Data sources are reliable, current, and valid, including properly defining and documenting Data elements in DSS-J (e.g., Data labels, properties and metadata, descriptions).

b. Provide Data that is accurate, complete, consistent, and ensure that the process is documented.

c. Each Source Agency Data Trustee is responsible for designating the appropriate individual to approve the migration of new Source Data into DSS-J. This individual should be

designated as the Data Trustee.

d. The Source Agency Data Trustee will also inform DSS-J IT regarding any CJI Data or otherwise sensitive Data: identifying which Data requires restricted access within the DSS-J, and who should or should not have access to that Data.

e. In some instances, a Member Agency may request the migration and addition of new Source Data to existing DSS-J security groups. These requests are beyond the scope of the Policy Manual and will require separate agreements between the requesting and Source Agencies.

(ii) Responsibilities of Source Agency IT

a. Provide Data that accurately represents what is in the Source Agency's own system.

b. Provide Data that is transmitted securely, regularly, and correctly to DSS-J.

(iii) Responsibilities of DSS-J IT

a. Ensure daily that the Data is uploaded correctly into the applicable DSS-J Staging Area (see Article III below).

b. Notify Identified Users immediately when uploads fail or other problems are detected.

c. Assign a unique DSS-J identification number to each record.

d. Create standards and procedures to reach a certain level of Data quality based upon how the Data is monitored, cleansed, and enriched ensuring such standards and procedures meet the requirements of Article III of this Policy Manual.

e. Upon request, provide DSS-J Operations with usage metrics and uptime statistics; and,

f. Maintain a Data dictionary (in consultation with the Source Agency's Data Steward).

(iv) Sealed Records. Expunged or otherwise sealed court records are removed from DSS-J daily.

a. OJD, as the Source Agency, for court records, produces a daily list of all cases that have been expunged or otherwise sealed after those cases were uploaded to the DSS-J.

b. OJD uploads the list of expunged or otherwise sealed after those cases to the DSS-J.

c. Per automated processes within DSS-J, the list is imported to the staging environment and any Data from any of cases that are on the list of expunged or otherwise sealed records is deleted from the DSS-J.

d. Within 24 hours after the list is imported and required Data deleted, the staged Data will overwrite the existing Data in the DSS-J.

Article II. User Management

Section 2.01 Requests for DSS-J Access

(a) Requester, or requester's employer, must have become a Member Agency by entering into an agreement with Multnomah County, which agreement shall be substantially in the form attached as **Appendix E** ("IGA").

(b) CJIS clearance is first required for all Identified Users prior to granting access. All Identified Users must maintain CJIS clearance through routine recertification.

(c) Requester must then fill out and sign the DSS-J Access Request Form. As part of completing the Access Request Form, the Requestor must agree to comply with the terms of this Policy Manual and its Member Agency's IGA.

(d) Prior to submitting the DSS-J Access Request Form, it must be approved by the requester's supervisor. The requester's agency must have at least one operations-level representative on the

DSS-J Operations Team.

(e) The requester or their supervisor must then submit the signed form by email to the DSS-J IT staff. The DSS-J IT staff will forward the request to the full DSS-J Operations Team for review.

(f) Requests for user access submitted by individuals or agencies without representation on the DSS-J Operations Team (see **Appendix B**) can be made by bringing the proposal to a DSS-J Operations Team meeting for discussion. The Operations Team will refer requests from these external requesters with a recommendation to the DSS-J Policy Team for review and approval.

(g) DSS-J Source Agencies may require routine internal audits of their own DSS-J Source Data. Auditors who require access to DSS-J will be required to submit an Access Request Form following the steps outlined in this section.

Section 2.02 Approval of DSS-J Access Requests

(a) Approval of an Identified User's access request may be granted electronically via email or at a DSS-J Operations Team meeting. The Identified User's approval must be documented either via email or through the DSS-J Operations Team minutes.

(b) DSS-J Data is segmented into groups by each Source Agency and access will be granted only to the Data segment approved by the corresponding Source Agency.

(c) The DSS-J Operations Team is responsible for following up with approvers to ensure that requests are approved within a reasonable timeframe.

(d) The DSSJ Operations Team shall provide the DSS-J IT team with the details for the approved Individual User, their necessary account information, and confirmation of the approval in order to create access.

Section 2.03 Granting Physical Access

(a) Access to DSS-J AD groups will be granted individually, with approval required by the Source Agency responsible for the AD group in question (e.g., MCDA must approve an Identified User's request to access Data housed in the DSS-J_AD_HOC_MCDA group).

(i) Multnomah County Sheriff's Office: MCSO Security Group (DSS-J_AD_HOC_MCSO)

(ii) Multnomah County District Attorney: MCDA Security Group (DSS-J_AD_HOC_MCDA)

(iii) Oregon Judicial Department: Court Security Group (DSS-J_AD_HOC_COURT)

(iv) Multnomah County Department of Community Justice: DCJ Security Group (DSS-J_AD_HOC_DCJ)

(v) DSS-J IT: DSS-J Security Group

(b) DSS-J IT will grant access once all Source Agency approvals are completed.

Section 2.04 New Identified Users shall:

(a) Read and affirm understanding of this Policy Manual and their Member Agency's IGA with their supervisor.

(b) Perform due diligence in receiving the proper training necessary to access and use DSS-J, as appropriate.

(c) Seek advice from supervisors and DSS-J Source Agencies regarding any DSS-J policy, practice, and information-sharing expectation.

Section 2.05 Review

(a) At each Operations Meeting, DSS-J IT will be prepared to share a report on who has access to each Member Agency's Data based on the current security model.

Article III. Data Use Roles & Responsibilities (see also Section 1.02 Governance Structure, Roles and Responsibilities)

Section 3.01 Purpose of Section

To set quality standards that must be in place to generate reports and products using the Data located in DSS-J. These quality standards provide the framework for how Data is collected, managed, stored, and retrieved within the DSS-J, including:

(a) Assuring the quality of the reports and information products generated from the Data in DSS-J (Quality Control); and

(b) Assuring the quality of the Data in DSS-J (Quality Assurance).

For a list of responsibilities related to Data quality control and assurance and the group responsible for each task see **Appendix D**.

Section 3.02 Inform and Approval Process for New Data Requests

(a) The process to inform a Source Agency of a request to use their Data:

(i) Using the DSS-J Project Notification Form, Identified Users will provide the following information to the Source Agency Data Steward at the commencement of the project and prior to the use and analysis of the Data:

a. The research question(s) to be answered;

b. The requestor and intended audience;

c. The Data requirements such as sources, variables, query parameters, and joins to other Data sources;

d. The assumed complexity of the project;

e. The intended methodology;

f. Whether Data validation is expected; and

g. Confirmation that Data use is permitted by law.

(ii) Upon receiving notification of a project using Source Agency's Data, it is the Source Agency's responsibility to:

a. Respond to Identified User's request and confirm receipt.

b. If use of Data is approved by Source Agency, Source Agency will:

i. Make resources available to accomplish the project, as practicable, and vetted by Source Agency policy representatives as needed.

ii. Provide Identified Users with available documentation as practicable.

iii. Review project documentation, as appropriate, and provide feedback throughout the course of the project.

c. Approval of requests to use Source Agency Data is in the sole discretion of the Source Agency.

d. Failure to obtain approval prior to use and analysis of the Data shall be considered a material breach of this Policy Manual.

(b) If the requester is a non-Source Agency Identified User, there is a heightened requirement that the requester will more frequently check in with Source Agency analysts from each Data source in use to ensure that their understanding of the Data is accurate, and that their analysis is on track to produce accurate results.

(c) The process to obtain approval to disseminate results:

(i) It is the Identified User's responsibility to share with the Source Agency any findings or reports/conclusions that rely on the Source Agency's Data prior to dissemination. Failure to share such findings or conclusions and obtain approval prior to dissemination shall be considered a material breach of this Policy Manual.

(ii) The Source Agency may:

a. Provide a QC check on conclusions with assistance from subject matter experts.

b. Review Data/conclusions with others who have a stake in the results.

(d) If the Source Agency does not provide approval to the requester to use the Data or to disseminate results, the requester may:

(i) Notify the designated DSS-J Policy representative from their agency to seek resolution.

(ii) If a resolution still cannot be met, the issue may be brought to the DSS-J Policy Team for discussion.

(iii) The DSS-J Policy Team cannot vote to overrule the Source Agency's decision. Unless the Source Agency approves the request to use the Data or to disseminate results, the requester may not do so.

Section 3.03 Quality Control: Data Analysis Performed by Identified Users

(a) **Purpose:** Retrieving and analyzing Data by an Identified User requires that the Identified User take steps to ensure that the Data is accurate, and the analysis and interpretation of the Data is correct.

(b) As required by Section 3.02(b) above, each Identified User shall frequently check in with Source Agency analysts from each Data source in use and ensure they are the use, analysis and interpretation of the Data is correct. Without limiting the prior sentence, at the commencement of each project, Identified User shall work with the Source Agency analysts from each Data source in use and determine how frequently Identified User shall check in with such Source Agency analysts.

Section 3.04 Quality Assurance

(a) Purpose: To ensure the underlying Data used in reports and products are accurate and to promote the highest possible quality assurance and quality control.

(b) Each Source Agency that contributes Data to DSS-J will perform periodic review to ensure the accuracy of their contributed Data in comparison to the Source Agency's own systems.

(i) With input from the DSS-J User Group, a list of agreed-upon fields will be checked against data contained in the Source Agency data systems.

(ii) Typical examples of Data to be reviewed include:

a. Changes in source system data;

b. New programs or business processes; or

c. Master data sets, both new and maintaining existing

i. Representatives from the Source Agency will brief the DSS-J User Group on the findings of their review.

ii. Sub-committees may be formed to address specific Data issues or decisions. The recommendations crafted by these groups will be presented to the DSS-J User Group.

Section 3.05 Correcting Inaccuracies

(a) In the event that the quality control measures outlined in the Policy Manual were followed and all requirements met, but inaccuracies are reported:

(i) Have a discussion at the User Group to identify the problem and come to a consensus about how to address the problem and prevent it in the future.

(ii) Depending on the type of error and resolution needed, the User Group will make a recommendation to Operations and/or the Policy Team for fix/response.

Section 3.06 Preventative

(a) Identified Users are required to abide by this Policy Manual and their Member Agency's IGA.

Section 3.07 Ongoing

(a) Identified Users are required to review this Policy Manual on an annual basis. DSS-J IT will monitor usage and remind Identified Users via email to review the Policy Manual every July 1st. The Identified User will include direct supervisor in the email response and indicate when this Policy Manual has been reviewed.

(i) Identified Users will have their access to AD groups suspended if they do not use DSS-J in a six-month (6) period. Identified Users will be removed from the DSS-J system entirely if they do not access the DSS-J in a twelve (12) month period.

Section 3.08 Proactive

(a) The proactive responsibility to ensure quality DSS-J use and reporting is up to each Individual User and Member Agency.

(b) Quarterly, the DSS-J IT team will review Identified Users and provide a report to the DSS-J Operations Team.

(c) Yearly on July 1st, the DSS-J Operations Team will review the Quality Assurance/Quality Control sections of this Policy Manual.

Section 3.09 Reactive

(a) If an Identified User violates any part of this Policy Manual:

(i) Impacted agencies will be notified;

(ii) Applicable agency supervisor(s) will be notified;

(iii) Identified User's Member Agency will follow own personnel processes, as applicable and appropriate;

(iv) As required, other notification procedures (HIPAA, CJIS) will be followed; and

(v) The Identified User's DSS-J access will be immediately and indefinitely suspended, pending the findings of an inquiry into the documented violation.

(b) Recommendations for removal/changes of access will go to the Policy Team representative for the Source Agency(ies) impacted by the violation.

Section 3.10 Consequences for Violating DSS-J Policies

(a) If an Identified User is found to have violated any DSS-J Policy, consequences may include additional DSS-J training or permanent termination of access to the DSS-J based on the results of an investigation.

Section 3.11 Policy Manual Review

(a) Biannually the entire Policy Manual will be reviewed by the Operations Team. Any recommendations for revisions to the Policy Manual will be forwarded to the Policy Team for review and consideration.

(b) Any changes proposed to this Policy Manual must be approved by unanimous consent of all Source Agencies.

Article IV. Database Structure and Access to DSS-J Data

Section 4.01 Purpose of Section:

Because the Data contained within the DSS-J includes law enforcement, sensitive and CJIS-protected Data, there are strict rules concerning access and sharing of the Data, both at the aggregate/summary and individual levels. The Data contained in the DSS-J warehouse represents a shared responsibility among the Member Agencies. Access control provides the mechanisms to restrict reading, writing, processing, and transmission of DSS-J Data. Therefore, this Policy Manual describes the shared vision of the need for confidentiality, integrity, and availability of DSS-J Data. It is the responsibility of all agencies covered under this Policy Manual (all agencies who contribute to and access DSS-J) and the individual Member Agency IGAs to ensure the protection of DSS-J Data between Member Agencies and the user community.

Section 4.02 DSS-J Structure

(a) **DSS-J Data Mart:** The DSS-J Data Mart is a central database where approved DSS-J Data is integrated from a Source Agency's enterprise data system.

(b) **Staging layer:** Used to validate the Data after it is migrated to DSS-J from the Source Agency's own system.

(i) Only DSS-J IT and the designated representative from the Source Agency have access to the Source Agency's Data in the staging layer. The Source Agency has the exclusive authority to determine if/when to migrate Data from the Staging layer to other layers.

(c) **Transformation/Integration layer**: Source Agency's own system business process rules are incorporated into the Data here.

(i) Only DSS-J IT and a representative from the Source Agency have access to the Source Agency's Data at this level. The Source Agency has the exclusive authority to determine if/when to migrate Data from the Transformation/Integration layer to other layers.

(d) **Reporting layer:** This is where Identified Users work with the Data from the Source Agencies. Data sets and views are built in this layer, and user acceptance testing (UAT) occurs here.

(e) Data may be imported into the Staging layer of DSS-J without migrating it up to the Transformation or Reporting layers.

Section 4.03 General Security Requirements

(a) In order to fulfill all general security requirements to maintain DSS-J access, the Identified User must:

(i) Maintain CJI Data clearance and receive a refresher security training at least every two years

(ii) Use a password to access that is 8 characters minimum, including a combination of three of the four: upper case, lower case, number, and special character

(iii) Agree to not share passwords.

(iv) Change his/her password every 90 days, per CJIS requirements.

Section 4.04 General Prohibitions

(a) Identified User shall not:

(i) decompile, disassemble, or otherwise reverse engineer DSS-J or attempt to discover its source code, underlying ideas, algorithms, files, or programming interfaces; and

(ii) attempt to re-identify Anonymized Data or Aggregated Data.

Section 4.05 Data Sharing

(a) Identified Users may share Datasets with other approved Identified Users if the intended recipient also has approved access to the AD group from which the shared Data originates and the sharing is consistent with the scope of the original approval form (e.g., MCSO shares a compiled Dataset with OJD that comes from a DCJ security group and OJD also has approval to access DCJ's Data).

(i) If using email, the Identified User should always send Data via secure email.

(b) Identified Users shall contact the Source Agency's Data Steward with any questions that arise while working with that Source Agency's Data, and/or comply with the quality control requirements covered in Article III: Data Use Roles & Responsibilities

(c) Identified Users shall inform the Source Agency and obtain Source Agency approval before applying for grants that require or involve the use of that Source Agency's Data, or offering to provide another Source Agency's Data for any analysis or project.

Section 4.06 Public Records Requests

(a) Any record requests that pertain to DSS-J may be subject to application of the Public Records Law, per the Member Agency's IGA. All agencies agree to participate in public records requests using DSS-J Data as outlined in the IGA, section 11.

Appendix A: DSS-J Governance Bodies: Roles and Responsibilities

Governance Body	Participants (role or person or designee)	Responsibilities
Policy Team	● LSPCC ED ● LPSCC PM ● Sheriff ● DCJ Director ● DA ● PPB Chief ● TCA/courts ● Mayor's Office/City	● Identify and define business problems ● Develop research questions ● Review and approve requests for Non-Member Agencies as outlined in this Section 1.02(a)(iii). ● Consider requests for DSS-J access made Non-Member Agencies and decide the appropriate course of action for formal approval of new DSS-J Member Agencies ● Define processes around access and use of DSS-J ● Define/confirm priorities ● Acknowledge DSS-J project milestones ● Work with appropriate Member Agencies to develop MOUs/IGAs, as needed ● Act as executive sponsors, as required per project. Executive Sponsors: ○ Get resources ○ Define/confirm priorities ○ Remove barriers ○ Acknowledge milestones
Operations Team	● OJD IT Supervisor ● Multnomah County Senior Development Analyst ● DCJ Research and Planning Manager ● Deputy District Attorney ● MCSO Director of Planning and Research ● DCJ IT Manager	● Governance and operational oversight as outlined in this Policy Manual; ● Review and approve DSS-J access requests made by Identified Users representing Member Agencies (see Appendix B); ● Receive and review outside agency access requests; ● Provide recommendations to the Policy Team; ● Establish DSS-J business processes and procedures that comply with this Policy Manual; ● Facilitate vertical communication across DSS-J system partners; ● Plan and facilitate Policy Team meeting agenda items, as appropriate; ● Brief Policy Team Members on issues, as needed; ● Receive and prioritize project requests and communicate priorities back to the appropriate DSS-J body; and ● Regularly review Identified User access.

User Group	• Agency analysts • Agency IT • DSS-J IT	• Identify DSS-J bugs; • Receive and prioritize low-level DSS-J requests that have been reviewed and approved by the Operations Team (e.g., small projects); • Brainstorm research questions; • Maintain training documents, DSS-J schema, and Data dictionaries; and • IRB considerations for research involving human subjects that potentially includes Data from multiple members; • Conduct Data analysis and complete Data-related projects, as prioritized. See Articles 3.02 through 3.06 and Articles 4.04 through 4.06 for rules related to Data access, use and analysis.

Appendix B: DSS-J Governance Roles

Agency	Data Trustee	Data Steward	Agency Policy Representative	Contribution
Multnomah County District Attorney	Assigned DDA/or IT Director	IT Director or designee	District Attorney	Source and Member Agency
Oregon Judicial Department	IT Manager	OJD assigned researcher or analyst designee	Trial Court Administrator	Source and Member Agency
Multnomah County Sheriff's Office	IT Manager	Director of Planning and Research	Sheriff	Source and Member Agency
Local Public Safety Coordinating Council	Assigned Data staff	Assigned Data staff	Executive Director, LPSCC	Member Agency
Department of Community Justice	Research and Planning manager	Research and Planning manager	DCJ Director	Source and Member Agency
Portland Police Bureau	Strategic Services manager	Assigned SSD staff	Chief of Police	Member Agency
Gresham Police Department	N/A	N/A	Chief of Police	Member Agency

Appendix C: DSS-J Data Elements of Interest

DSS-J PII elements:

1. Last, First, Middle Name
2. Date of Birth
3. Address, City, State, Zip
4. Social security numbers
5. Fingerprint classification number
6. ID cards: Oregon ID number, Oregon driver's license number, Washington DL number, Washington ID number

DSS-J CJIS elements:

1. Oregon SID
2. FBI Number
3. Fingerprint classification number
4. Social security numbers
5. Mug ID
6. Oregon Driver's License
7. Washington Driver's License
8. Washington ID Card

Appendix D: DSS-J Data Elements of Interest

Data Quality Responsibility	Group or Persons Responsible
Ensuring Data entry accuracy	Source Agency Data entry
Sending accurate Data to DSS-J	Source Agency IT
Ensuring Data in DSS-J was accurately translated	DSS-J IT working with Source Agency IT
Ensuring Data drawn from DSS-J is complete and accurate	Analysts obtaining the Data working with Source Agency analysts
Ensuring analytic conclusions are accurate	Analyst(s) from Source Agency(ies)
Ensuring relevant permissions are acquired	Data Stewards and Analyst(s) obtaining the Data
Notify Source Agency of Data use and methodology	Data Stewards and Analyst(s) obtaining the Data

Appendix E: DSS-J IGA Form

INTERGOVERNMENTAL AGREEMENT
Decision Support System – Justice (DSS-J)
Agreement Number: [insert contract number]

This INTERGOVERNMENTAL AGREEMENT ("Agreement") is between MULTNOMAH COUNTY, a political subdivision of the state of Oregon ("County"), acting through its Local Public Safety Coordinating Council (LPSCC), the Multnomah County Sheriff's Office (MCSO), the Multnomah County District Attorney's Office (MCDA), and the Department of Community Justice (DCJ) (LPSCC, MCSO, MCDA, and DCJ are collectively referred to as "Host Agencies"), and _____ ("Member Agency"). The effective date of the Agreement will be the date on which all Parties have signed the Agreement ("Effective Date").

RECITALS

WHEREAS, Host Agencies and Member Agency are Criminal Justice Agencies;

WHEREAS, County has developed, owns, and maintains the Information Systems comprising Decision Support System-Justice (DSS-J), a data warehouse used, in part, to store CJI contributed by the Host Agencies and other Criminal Justice Agencies;

WHEREAS, the Parties wish to contribute the Data including, without limitation, CJI set forth in **Schedule A** to DSS-J and for their Identified Users to have access to DSS-J, subject to the conditions and policies set forth herein or incorporated by reference;

WHEREAS, the Parties wish for the Data including, without limitation, CJI they contribute to DSS-J to be accessed and otherwise used by Identified Users, subject to the conditions and policies set forth herein or incorporated by reference; and

WHEREAS, federal and state laws limit access to and the use of certain CJI and require Criminal Justice Agencies to enter into particularized written agreements when they share or disseminate certain CJI.

NOW THEREFORE, in consideration of the above Recitals which are incorporated into the Agreement and mutual promises below, the Parties agree as follows:

AGREEMENT

1. **Definitions**. Terms used, but not otherwise defined in this Agreement, will have the same meaning as those terms as defined in the DSS-J Policy Manual. A reference to a regulation means the section as in effect or as amended, and for which compliance is required.

a. "Administration of Criminal Justice" is defined in the Security Policy and means the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of

criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

b. "Anonymized Data" is Data from which the following data types and elements have been removed: (i) PII; (ii) nonconviction data, as defined in 28 CFR § 20.3(q); (iii) NCIC restricted files, as described in the Security Policy at section 4.2.2; and (iv) any other Data marked or tagged RESTRICTED, as described below, by a Criminal Justice Agency. Anonymized Data is not CJI.

c. "Authorized Use" is use of Data including, without limitation, the use of CJI for the Administration of a Criminal Justice function, and is otherwise consistent with the terms of the Agreement, particularly **Schedule A**, the Security Policy, and the Policy Manual attached as **Schedule B**.

d. "Authorized User" is defined in the Security Policy and means an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

e. "Breach" is the acquisition, access, use, dissemination, or disclosure of Data that violates the Security Policy, the Agreement, the Policy Manual, or compromises the security or privacy of such information.

f. "Involved Persons" are persons involved in a case or proceeding related to the investigation of a law violation, including defendants, victims, witnesses, and any identified relatives or associates thereof.

g. "Loss" and "Losses" means any claim, damage, loss, liability or expense including, without limitation, fines, and judgments suffered directly or by reason of any act, omission, claim, or Proceeding.

h. "Party" refers to each of the Host Agencies and the Member Agency.

i. "Parties" refers, collectively, to all of Host Agencies, and Member Agency.,

j. "Policy Manual" refers to the DSS-J Policy Manual that is attached to this Agreement as **Schedule B**.

k. "Proceeding" means any actual, threatened, pending or completed dispute, investigation, or inquiry, whether civil, criminal, administrative or investigative, implicating a matter arising under or related to the Agreement.

l. "Public Records Law" means the Oregon Public Records Law, including ORS 192.311 to 192.475, the provisions for the Custody and Maintenance of Public Records, ORS 7.110, 8.125, and 192.005 to 192.170, and laws incorporated by reference.

m. "Record" means information prepared, owned, used, or retained by either Party, and pertaining to their respective operations and business related to the Agreement, that is inscribed on a tangible medium, commonly a document, or that is stored in an electronic or other medium and is retrievable in perceivable form. Record includes, a disclosing Party's Data.

n. "Security Policy" means version 5.9 of the Criminal Justice Information Services Security Policy, CJISD-ITS-DOC-08140-5.9.

2. **Policy Manual.** The Parties acknowledge the value in collaborating and participating in the DSS-J. In furtherance of supporting participation, the Parties agree that any access to and use of Data from the DSS-J shall comply with the terms, policies and processes set forth in the Policy Manual and this IGA. The Parties agree that any revisions to the Policy Manual that affect access to and use of Data from the DSS-J must be approved by the Parties to this Agreement.

3. **Term and Termination**.

a. **Term**. The term of the Agreement shall begin on the Effective Date and continue for four (4) years. Unless terminated as provided herein, the Agreement term shall automatically renew for successive two year terms.

b. **Termination**. The Agreement may be terminated as follows.

i. **Termination for Convenience**. Either Party may terminate this Agreement by providing at least thirty (30) days prior written notice of such termination to the other Party.

ii. **Termination for Default**. Either Party may immediately terminate this Agreement after providing written notice, as set forth in **Section 16**, of the other Party's failure to comply with any of the provisions of this Agreement. To avoid ambiguity, a Party may immediately terminate the Agreement under this **Section 3(b)(ii)** upon: (A) any Breach of the terms of this Agreement; and (B) if, after receiving notice and an opportunity to cure as provided in **Section 16**, a Party fails to comply with the Agreement and all applicable federal and state laws governing access to and use of DSS-J and CJI.

c. **Effect of Termination**. Member Agency's termination of the Agreement shall result in its loss of access to DSS-J. Except as allowed under this subsection, upon termination of this Agreement for any reason, Hosting Agencies and all other Member Agencies shall immediately stop all current and future use of any Data contributed by the terminating Member Agency. To the extent allowed by applicable law, Hosting Agencies shall either return to Member Agency or destroy all Data that was contributed by Member Agency. Data from Member Agency that consists only of Anonymized Data or Aggregate Data and that, prior to termination and consistent with requirements of the Policy Manual, had been incorporated into a report or other analysis may be retained and continued to be used in that report or analysis.

Upon termination of this Agreement for any reason, the Parties will extend the protections of this Agreement to any Data that they are required to retain under any provision of this

Agreement. The terms of this Agreement will remain in effect until all Data provided by a Party to the other, or created or received by a Party on the other Party's behalf, is destroyed or returned; or, if it is infeasible to return or destroy Data, protections are extended to such information, in accordance with the termination provisions in this section. To avoid ambiguity, the Parties' obligations under this **Section 3(c)** will survive termination of the Agreement.

4. **CJI Contributed to DSS-J**. The Parties shall limit CJI contributed to DSS-J as follows.

a. **Data Classification**. All Data files contributed to DSS-J shall be tagged with one of the following classifications. For CJI the contributing Party believes: (i) is subject to public inspection under ORS 192.345(3), or should be made public via the authority granted under 28 CFR §§ 20.20(c) or 20.33(c), the file(s) shall be tagged "PUBLIC"; or (ii) is not subject to public inspection, the files shall be tagged "RESTRICTED."

b. **Prohibited CJI**. The Parties shall use commercially reasonable efforts to ensure that no CJI is contributed to DSS-J that contains information: (i) originating from a NCIC restricted file, as described in the Security Policy at section 4.2.2; (ii) concerning a Ward of Oregon Juvenile Court, as those terms are defined in, ORS 419A.004, unless CJI concerning the Ward has been made publicly available ORS 419A.255(5)-(6); (iii) that is nonconviction data, as defined in 28 CFR § 20.3(q), unless the contributing Party has determined that disseminating such CJI is permitted under 28 CFR § 20.21(b); (iv) Biometric Data protected under ORS 181A.220; and (v) presentence and probation reports under ORS 137.077 and 137.530.

5. **Access to and Use of DSS-J and Data**. The Parties shall limit access to DSS-J to Identified Users. The access and use of Data shall be limited to Authorized Users and Authorized Uses. The Parties, on their behalf and on behalf of their Identified Users, warrant and represent they will follow the terms, policies and processes set forth in the Policy Manual and this IGA.

6. **Licensing and Ownership of Data**. Subject to compliance with the terms and policies set forth in **Schedule B**, the Parties grant and receive the following licenses.

a. **DSS-J License**. County grants to Member Agency a fully paid, revocable, non-exclusive, royalty-free license to access and use DSS-J for activities related to the Administration of Criminal Justice, and to authorize its Identified Users to do the same on Member Agency's behalf. County reserves all rights in DSS-J not expressly granted to Member Agency.

b. **CJI Cross License**. Each Party grants to the other a fully paid, revocable, non-exclusive, royalty-free license to access the Data they contribute to DSS-J, including to make, reproduce, and prepare derivative works based thereon, and to perform, display, and distribute copies of such Data or derivative works thereof, and to authorize others to do the same on their behalf, as permitted by law and as consistent with the terms and policies in **Schedule B** and as allowed under the terms of this Agreement. Each Member Agency reserves all rights in the Data it contributes to DSS-J that are not expressly granted to County or other Member Agencies.

c. **Sublicensing**. Member Agency grants to Host Agencies the right to allow other Criminal Justice Agencies to access and use Member Agency's Data under the same terms contained in the Agreement including, without limitation, the Policy attached as **Schedule B**. As applicable, each Party is responsible for obtaining authorization and consent from any Involved Person before contributing any PHI to DSS-J.

d. **Cross License for Anonymized Data**. Each Party grants to the other, and to all Criminal Justice Agencies authorized to access DSS-J, a fully paid, revocable, non-exclusive, royalty-free license to use Anonymized Data, including to make, reproduce, and prepare derivative works based thereon, and to perform, display, and distribute copies of such Anonymized Data or derivative works thereof, and to authorize others to do the same on their behalf. Provided, however, use of Anonymized Data shall be consistent with the policies set forth in **Schedule B**.

e. **Ownership**. Unless otherwise specified in writing, all Data will remain the property of the disclosing Party. Nothing contained in this Agreement will be construed as a grant of any right or license or an offer to grant any right or license by either Party to the other, or any other Criminal Justice Agency, with respect to the Data exchanged hereunder. All Data (including all copies thereof) shall be destroyed or returned to the disclosing Party upon the request of the disclosing party or termination of the Agreement, as set forth in **Section 3(c)**.

7. **Responsibilities of the Parties**.

a. **Host Agencies' Responsibilities**. Host Agencies shall:

i. Use reasonable efforts to provide a daily or weekly upload to DSS-J of the Data set forth in **Schedule A**.

ii. Enable access to DSS-J for Member Agency's Identified Users as set forth in **Schedule A**.

iii. Ensure appropriate technical safeguards are used to protect DSS-J and Data, including mechanisms that: (A) prevent Data from being modified, destroyed, accessed, changed, purged, or overlaid in any fashion without authorization; (B) prohibit inquiry, record updates, or destruction of records, by any Identified User other than Identified Users who are authorized to make such changes; (C) limit destruction of Data to designated Identified Users or processes under the direct control of County IT administrators responsible for maintaining DSS-J; (D) detect and store for the output of designated representatives of the Parties all unauthorized and unsuccessful attempts to access DSS-J; and (E) ensure an audit trail is created that preserves information on the mechanisms listed in this **Section 7(a)(iii)(A)** through **(D)**.

iv. At Member Agency's written request, remove from DSS-J any Data contributed by Member Agency that Member Agency has identified with specificity for removal.

v. Provide to Member Agency's IT professionals the IT maintenance and support services described in **Section 8**.

vi. Develop and maintain an updated and accurate list of all Host Agencies' Identified Users and require all other Criminal Justice Agencies accessing DSS-J to periodically provide to Host Agencies a similar current list of Identified Users.

vii. Comply with all applicable federal and state laws and regulations relating to the use, disclosure, and the maintenance of the Data including, without limitation all applicable requirements the Oregon Consumer Information Protection Act (ORS 646A.600 et. seq.) and all applicable requirements of the Security Policy with respect to CJI.

viii. Ensure that its employees and representatives comply with the requirements of this Agreement and the Policy Manual.

ix. Take immediate steps to stop an unauthorized use or disclosure of Data and cure the Breach, if such event occurs.

x. Require any other Criminal Justice Agency that will access DSS-J to enter into an agreement whose terms are substantially identical to those in this Agreement prior to such access.

b. **Member Agency's Responsibilities**. Member Agency shall:

i. Use reasonable efforts to provide transfers to County of the Data set forth in **Schedule A** on at least a weekly basis.

ii. Ensure appropriate technical safeguards are used to protect its Data transferred to County, its Information Systems, and any Data from DSS-J stored by Member Agency.

iii. Develop and maintain an updated and accurate list of all Member Agency's Identified Users and provide County with a copy of such as provided in **Schedule B**.

iv. Comply with all applicable federal and state laws and regulations relating to the use, disclosure, and the maintenance of Data including, without limitation all applicable requirements the Oregon Consumer Information Protection Act (ORS 646A.600 et. seq.) and all applicable requirements of the Security Policy with respect to CJI.

v. Ensure that its employees and representatives comply with the requirements of this Agreement and the Policy Manual.

vi. Take immediate steps to stop an unauthorized use or disclosure of Data and cure the Breach, if such event occurs.

8. **Maintenance and Support**. County will provide to Member Agency information regarding such IT requirements, procedures, instructions and other documents regarding the methods available for accessing DSS-J and generating reports from Data therein.

a. **DSS-J System Maintenance**. As needed and in its sole and absolute discretion, County will perform periodic or routine modifications to DSS-J and the IT systems supporting it to improve or maintain the system's existing functionality. Such modifications include bug fixes and testing to ensure compatibility with subsequent or complementary products or services.

b. **Identified User Help Line**. County will provide a help line during normal business hours for Identified Users to report problems with DSS-J and seek assistance with basic usability issues and questions, such as: operator errors; account creation, setup, or access questions.

c. **Member Agency Training**. County may provide Member Agency with training materials to enable Member Agency's IT professionals to provide DSS-J training and instruction to Identified Users. County shall provide to an Identified User designated by Member Agency such instructions, documents, and training necessary to enable that individual to perform limited administrative functions such as resetting passwords.

d. **Service Continuity**. By the Effective Date, County will have a business continuity plan in place and will evaluate the IT disaster recovery portion of such plan at least annually. The plan must address procedures for response to emergencies and other business interruptions. Specifically, the plan must demonstrate that, in the event of a disaster or other service or business interruption, County has provided for: (i) backing up and storing DSS-J Data at a location that is sufficiently remote from the facilities at which it is hosted in case of loss of that Data at the primary site; (ii) rapid restoration, relocation, or replacement of resources associated with DSS-J; (iii) short and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to DSS-J; and (iv) reviewing, testing, and adjusting the plan based on its at least annual evaluation.

9. **Disclaimers**. The Parties acknowledge and agree that DSS-J is not designed nor tested for a level of reliability suitable for use in any information system the failure of which can reasonably be expected to cause injury to persons or property. Similarly, the Parties do not warrant that Data will meet the requirements of any other Criminal Justice Agency or Identified User, or that any of this information will be accurate. DSS-J, Data may contain bugs and inaccuracies and the Parties can and should expect errors, anomalies, and incorrect results under normal use. The Parties agree to take precautions to offset these risks and to not use the DSS-J Data where personal injury or property damage may result. DSS-J, DATA ARE PROVIDED "AS IS". NEITHER PARTY MAKES ANY WARRANTIES, CONDITIONS OR UNDERTAKINGS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

10. **Proceedings.**

a. **Notice**. If any third-party institutes a Proceeding against a Party (the "Notified Party") alleging a tort, as now or hereafter defined in ORS 30.260, and related to a performance under the Agreement (a "Third-Party Claim"), the Notified Party shall promptly notify the other Parties in writing of the Third-Party Claim and deliver to the other Parties, along with

the written notice, a copy of the claim, process and all legal pleadings with respect to the Third-Party Claim that have been received by the Notified Party. Each Party is entitled to participate in the defense of a Third-Party Claim, and to defend a Third-Party Claim with counsel of its own choosing. Receipt by the other Parties of the notice and copies required in this section and a meaningful opportunity for the other Parties to participate in the investigation, defense, and settlement of the Third-Party Claim with counsel of its own choosing are conditions precedent to each of the other Parties' contribution obligations under this **Section 10** with respect to the Third-Party Claim.

b. **Right of Contribution**. With respect to a Third-Party Claim for which one or more of the Parties are jointly liable (or would be if joined in the Third-Party Claim), each liable Party shall contribute to the amount of Losses paid in settlement actually and reasonably incurred and paid or payable by the other Parties in such proportion as is appropriate to reflect the relative fault of that liable Party on the one hand and any other liable Parties on the other hand in connection with the events that resulted in such Losses, as well as any other relevant equitable considerations. The relative fault of each liable Party on the one hand and of any other liable Parties on the other hand shall be determined by reference to, among other things, the Parties' relative intent, knowledge, access to information, and opportunity to correct or prevent the circumstances resulting in such Losses. Each Party's contribution amount in any instance is capped to the same extent it would have been capped under Oregon law if a local public body had sole liability in the proceeding.

11. **Requests for Records**.

a. **Public Records Law**. As custodians of Records under ORS 192.311(2), and public bodies responsible under ORS 192.318(2) and ORS 192.411(2) with responding to public records requests, the Parties acknowledge they must respond to public records requests concerning Records. Any Record request made that pertain to DSS-J, including this Agreement, may be subject to application of the Public Records Law.

b. **Responses to Records, Data Requests**. If a Party receives (the "Recipient") a subpoena, warrant, or other legal order, demand or request (collectively, a "Legal Demand") seeking Records or Data for which another Party is a custodian (as defined by Oregon law, the "Custodian"), the Recipient will promptly provide a copy of the Legal Demand to the Custodian along with copies of Records or Data in their possession that the Recipient believes responds to the Legal Demand. In the event of a Legal Demand the Parties agree to consult, cooperate, and collaborate with each other in their responses.

c. **Records, Data Subject to a Public Records Law Exemption**. In the event a Recipient receives a Legal Demand for Records or Data that the Custodian asserts is exempt from disclosure under the Public Records Law, prior to Recipient disclosing any Records or Data, Recipient shall first give Custodian sufficient notice and provide such information as may be reasonably necessary to enable Custodian to take action to protect its interests and its Records or Data. If Custodian elects to oppose disclosure of its Records or Data and seek a protective order or other similar remedy, Recipient will cooperate in good faith to the extent reasonably practicable with Custodian's efforts to protect its Records or Data.

d. **Injunctive Relief**. Each Party acknowledges that use and disclosure of its Records and Data not in accordance with this Agreement will cause irreparable injury to such Party. Accordingly, a Party may seek and obtain injunctive relief against use and disclosure of its Data in breach of the terms of this Agreement. The parties acknowledge and agree that the covenants contained in this Agreement are necessary for the protection of its interests and are reasonable in scope and content.

12. **Confidentiality**.

a. The Parties acknowledge and agree: (i) to exercise the same degree of care and protection, but no less than a reasonable degree of care and protection, over the other Party's Data as each Party exercises with respect to its own similar information; (ii) that all Data disclosed pursuant to the Agreement should be considered confidential and proprietary; (iii) not to use any Data during the Term and for as long as such Party has possession or control of any Data for any purpose other than as permitted under the Agreement or as required under law; (iv) not to disclose or provide any Data to any third-party, except as expressly allowed under this Agreement or required by law; (v) not to remove or destroy any proprietary markings on the Data; and (vi) to return or destroy all of the other Party's Data on the expiration or termination of the Agreement, unless prohibited by law. As requested, a Party shall certify to the other the destruction of any of the other's Data, as applicable, within its possession or control.

b. Subject to the requirement to follow all processes of the Policy Manual, the Agreement does not otherwise require the Parties to protect information that: (i) was known or readily ascertainable by proper means before being disclosed; (ii) is or becomes available to the general public without fault or action of either Party; (iii) is disclosed to either Party by a third-party that breaches no confidentiality obligation through that disclosure; (iv) is developed independently by either Party without reference to or use of Data; or (v) is required to be disclosed by law or to a government authority.

c. Disclosure by either Party of Data or CJI to its professional advisors, employees, agents, affiliates, subsidiaries, subcontractors, and consultants is authorized only to the extent: (i) such disclosure is necessary to enable the performance of its obligations under the Agreement; and (ii) such parties receiving Data are comparably bound to safeguard and keep confidential such information.

13. **Information Security**. Each Party acknowledges and agrees it has implemented appropriate risk management techniques, including administrative, technical, and physical safeguards, to protect and ensure continuity of access to information systems, Data, and Records. Without limitation, the technical safeguards will incorporate industry recognized system hardening techniques. The Parties will at least annually audit their safeguards to ensure all information systems within their respective control and involved in using, storing, maintaining, or transmitting Data, are secure and protect Data from unauthorized disclosure, modification, or destruction. Where a Party, or its employees, agents, third-party processors, or permitted subcontractors, have access to the other Party's Information System(s), Records, or facilities, the Party with such access will comply with the following:

a. **Security Undertaking**. Without limiting the obligation of confidentiality described in **Section 12**, the Parties will be responsible for establishing and maintaining an information security program that is compliant with all relevant federal and state laws and otherwise designed to: (i) ensure the security and confidentiality of Information System(s) and CJI and Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Information System(s) and Data; (iii) protect against unauthorized access, modification, or use of Information System(s) and Data; (iv) ensure the proper disposal of Data stored or exchanged on the Information System(s); and (v) ensure that all employees, agents, permitted subcontractors, and third-party processors, if any, comply with all of the foregoing.

b. **Access Controls**. Each Party will take necessary and reasonable precautions to appropriately limit access by their respective employees, agents, affiliates, subcontractors, and other representatives to the other Party's Information System(s) and Data. Without limitation, a Party with access to the other Party's Data shall:

i. restrict and control access to: Information Systems from which Data is uploaded to DSS-J; facilities housing paper documents containing Data from DSS-J; or Information Systems hosting software as a service (SaaS) used to process Data from DSS-J, including establishing and observing effective procedures for tracking access and chain of custody thereof;

ii. limit access to and use of Data from DSS-J to only the minimum Data necessary to accomplish the intended purpose of the access;

iii. limit the access, use, disclosure, and dissemination of Data to Authorized Uses and to those Authorized Users that need access to Data from DSS-J;

iv. require that all individuals prior to receiving access to DSS-J or Data from DSS-J to submit to and pass, based on the process and criteria set forth in OAR 407-007-0030 through 407-007-0060, a criminal history records check, or a substantively similar background check, that includes a state of residency and national fingerprint based record check; and

v. prevent Data from DSS-J from being loaded onto portable computing devices or portable storage components or media unless necessary under this Agreement and adequate security measures are in place to ensure the integrity and security of Data, including without limitation: (A) a policy on physical security for such devices to minimize the risks of theft and unauthorized access; (B) a policy prohibiting viewing Data in public or common areas; (C) ensuring all such portable computing devices have anti-virus software, personal firewalls, and system password protection; (D) ensuring the Data stored on portable computing or storage device or media is encrypted while stored on such device; and (E) creating and maintaining an accurate inventory of all such devices and the individuals to whom they are assigned.

14. **Right of Audit**. Each Party will have the right to review the other's information security program related to safeguarding access to and Data from DSS-J prior to the Effective Date and from time to time during the term, including to perform audits at the other Party's work site(s). In lieu of an onsite audit, a Party may complete an audit questionnaire provided by the other, which must be returned to the requesting Party within forty-five (45) days of the date the questionnaire was received.

15. **Breach Notification**. In the event of an actual or suspected Breach involving DSS-J, its Information System(s), or any Data from DSS-J, a Party will immediately notify the other of the Breach or suspected Breach and will comply with all applicable breach notification laws. Upon learning of a Breach, County shall immediately suspend access to the DSS-J for the Identified User(s) that are believed to be responsible for the breach. The Parties agree to cooperate in any Breach investigation and remedy of any such Breach, including, without limitation, complying with any law concerning unauthorized access or disclosure, as may be reasonably requested by a Party. Member Agency will send any applicable notifications regarding a Breach to the following notification email address: IT.Security@multco.us.

County will send any applicable notifications regarding a Breach to the following notification email address: Mul.Managers@ojd.state.or.us.

a. **Notification of Breach Experienced By non-Party**. The Parties acknowledge and agree that in the event either learns of an actual or suspected Breach involving DSS-J, or Data from DSS-J, and affecting a Criminal Justice Agency that has access to DSS-J but is not a Party hereunder, the Party will notify the other Party, and the affected Criminal Justice Agency of such breach.

16. **Breach of Agreement; Sanctions**. In the event of a breach of the Agreement, including a violation of a term or policy in **Schedule B**, County shall immediately restrict or prohibit access to DSS-J by the breaching Party and its Identified Users. Except as otherwise provided in **Section 3**, the breaching Party shall be notified in writing of such action and given ten (10) days in which to explain and cure the breach before reinstatement of access is considered. A breach of the Agreement regarding access to or use of Data shall be considered a material breach. The Parties agree that injunctive relief requiring specific performance would be appropriate relief for such a breach.

17. **Remedies in Event of Breach of the Agreement**. The Parties recognize that irreparable harm may result in the event of a breach of this Agreement. In the event of such a breach, the non-breaching Party may be entitled to enjoin and restrain the other from any continued violation. This **Section 17** shall survive termination of the Agreement.

18. **Dispute Resolution**. All Parties will, in good faith, cooperate with each other to assure that all disputes between the Parties will be resolved as expeditiously as possible. The process for resolving disputes shall be as follows:

a. Any dispute between the Parties shall be submitted for resolution to the Parties' respective contacts listed on **Schedule A**.

b. If the Parties' respective contacts are unable to resolve the dispute within five business days, the dispute shall be escalated for resolution by the Parties' respective leaders.

Nothing in this **Section 18** is intended to impair either Party's right to seek an injunction or other available relief as provided herein.

19. **Merger, Waiver**. This Agreement and all exhibits and attachments, if any, constitute the entire agreement between the Parties on the subject matter hereof. There are no understandings, agreements, or representations, oral or written, not specified herein regarding this Agreement. No waiver or consent under this Agreement binds either Party unless in writing and signed by both Parties. Such waiver or consent, if made, is effective only in the specific instance and for the specific purpose given. EACH PARTY, BY SIGNATURE OF ITS AUTHORIZED REPRESENTATIVE, HEREBY ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.

20. **Order of Precedence**. In the event of any inconsistency between any of the documents constituting the Agreement, the following order of precedence will apply: (a) **Schedule B**; (b) the terms and conditions in the body of the Agreement; and (c) **Schedule A**.

21. **Interpretation**. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits each party to comply with all relevant laws, including implementing regulations. The doctrine of *contra proferentem* may not be applied to the Agreement.

22. Survival. All rights and obligations cease upon termination or expiration of this Agreement, except for the rights and obligations and declarations which expressly or by their nature survive termination of this Agreement, including without limitation this Section 22, and Sections 3(c), 6(e), 9, 10, 11, 12, 13, 15, 16, 17, and 18.

23. **Miscellaneous**. Each Party represents and warrants that it has the power and authority to enter into and perform the Agreement. The Parties agree that each is an independent contractor of the other. This Agreement does not create any form of legal association that would impose liability upon one Party for any act or omission of the other, nor does it preclude either Party from conducting similar business with other parties. Except as otherwise provided above, the Agreement may only be amended or supplemented by a writing that: (a) is signed by a duly authorized representative of each Party; (b) clearly recites the Parties' understanding and intent to amend the Agreement; and (c) clearly and with specificity describes the terms to be amended or supplemented. The invalidity of any term or provision will not affect the validity of any other provision. The Agreement will be interpreted and enforced according to the laws of the state of Oregon.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

INTERGOVERNMENTAL AGREEMENT
Signature Page

The Agreement may be executed in multiple counterparts and may be electronically signed. Any verified electronic signatures appearing on the Agreement are the same as handwritten signatures for the purposes of validity, admissibility, and enforceability. Any reproduction of the Agreement made by reliable means is considered an original.

Multnomah County	**Member Agency**
By:	**By:**
_____	_____
Printed Name:	**Printed Name:**
_____	_____
Title:	**Title:**
_____	_____
Date:	**Date:**
_____	_____

Multnomah County Attorney Review:
Reviewed: JENNY M. MADKOUR, COUNTY ATTORNEY FOR MULTNOMAH COUNTY, OREGON

By:

_____
Assistant County Attorney

Date:

_____

SCHEDULE A
Authorized Uses

Party Contacts.

COUNTY	MEMBER AGENCY
Representative: _____ Address: _____ City, State, Zip: _____ Email: _____ Phone: _____ Fax: _____	Representative: _____ Address: _____ City, State, Zip: _____ Email: _____ Phone: _____ Fax: _____

County Data contribution.

DSS-J standardizes certain commonly used fields where discrepancies exist between member agencies. These fields include demographic fields, charge codes, charge modifiers, charge descriptions, certain crime and charge indicators (e.g. weapons, domestic violence), date formats, judge information, and sanction descriptions, among others. DSS-J contains all variations of a person's name that is recorded in each source systems. One name for each individual is identified as the True Name which can be used for reporting. All variations of past and present addresses are also stored.

Member Agency Data contribution.

MCSO: The Multnomah County Sheriff's Office contributes data from its SWIS data system. The data is related primarily to bookings/admissions but also includes fields for tracking certain in-custody events and statuses. Specific data elements include defendant identifiers, booking information (e.g. facility, dates, LEA identified offenses), warrants, interviews, sentences, custody releases, defendant demographics, as well as movements within and between facilities. DSS-J also produces a monthly snapshot of the in-custody population using data contributed by MCSO.

MCDA: The Multnomah County District Attorney's Office contributes data from its CRIMES data system. Specific data elements include defendant identifiers, defendant demographics, filed charges, charge descriptions, charge and case statuses, charge and case events, charge and case dispositions, corresponding dates, as well as victim identifiers (victim identifier is for aggregate purposes only. No personally identifiable information for individual victims is stored in DSS-J)

DCJ: The Multnomah County Department of Community Justice contributes data from its DOC data system related to client supervision. Specific data elements include client identifiers, client demographics, supervision type and status (active/not active), and supervision location.

OJD: The Oregon Judicial Department contributes publicly available data from its ODYSSEY data system. Specific data elements include publicly available defendant identifiers, defendant demographics, case party descriptions, case counts, case dispositions, case events, assigned judges, charge descriptions, charge types and statuses, court hearing events, hearing types, session names, calendar descriptions, hearing statuses, hearing results, sentencing types, dispositional departures, sentencing descriptions, sentence amendments, sentence conditions, sanction types, court fees and fines (does not include restitution), sanction durations, warrants, warrant charges warrant status, and corresponding dates for all relevant incidents.

Authorized Use(s). Access to and use of DSS-J and all Data therein is limited to the purpose(s) for which access to DSS-J was granted. See the applicable DSS-J User Access Request Form for details on each Authorized User's allowed access and allowed uses.

SCHEDULE B
DSS-J Policy Manual