

RESOLUTION NO. 1203

A RESOLUTION AUTHORIZING AN AMENDED INTERGOVERNMENTAL AGREEMENT WITH THE CITY OF PORTLAND, OREGON, FOR THE REGJIN PROJECT

WHEREAS, the City of Portland, Oregon has acquired a law enforcement Records Management System to maintain a multi-agency, multi-jurisdictional set of law enforcement applications and associated databases; and

WHEREAS, the primary objective of the region is to develop a shared common database available to cooperatively prevent criminal activity, track resource utilization, facilitate rapid and efficient communications, provide immediate and coordinated assistance among area agencies for day-to-day, tactical, and strategic operations, improve the ability of law enforcement to prevent and solve criminal activity through shared system functionality and cooperative operations, effectively prosecute criminals, and identify short and long term leveraging opportunities for cost effective infrastructure investments to meet regional requirements; and

WHEREAS, the City of Portland, Oregon, is inviting numerous Regional Partner Agencies to enter into an intergovernmental agreement for the user board of the Regional Justice Information System (RegJIN); and

WHEREAS, the City of Canby, Clackamas County, Oregon desires to be a participating Regional Partner Agency for the RegJIN Project; and

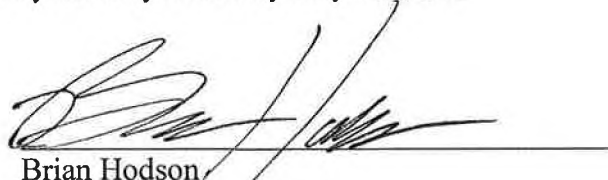
WHEREAS, the City of Canby, Clackamas County, Oregon has heretofore participated as a Regional Partner Agency for the RegJIN Project with the passage of Resolution 1183 on March 14, 2014.

NOW THEREFORE, IT IS HEREBY RESOLVED by the City of Canby as follows:

1. The City of Canby authorizes the Intergovernmental Agreement (“IGA”) with the City of Portland, Oregon, as amended, for participation in the RegJIN Project as described in the form attached hereto as Exhibit A.

This resolution shall take effect on November 19, 2014.

ADOPTED this 19th day of November 2014 by the City of Canby City Council.



Brian Hodson
Mayor

ATTEST:



Kimberly Scheafet, MMC
City Recorder

**RegJIN PARTICIPANT INTERGOVERNMENTAL AGREEMENT
REGIONAL PARTNER AGENCY – FULL ENTRY**

This Intergovernmental Agreement (“Agreement”) is made effective on 01-01-15 (“Effective Date”) by and between the City of Portland, a municipal corporation of the State of Oregon, and its successors or assigns (hereinafter referred to as “City”) and City of Canby (hereinafter referred to as “RPA”), a(n) municipal corporation, by and through their duly authorized representatives. Authority to enter into the Agreement is pursuant to Oregon Revised Statutes (“ORS”) 190.003.

This Agreement may refer to the City and RPA individually as a “Party” or jointly as the “Parties.”

This Agreement shall be perpetual and remain in effect unless otherwise terminated per the terms of this Agreement.

RPA Contact:

Chief Bret Smith

Canby Police Department

1175 NW 3rd Avenue

Canby, OR 97013

City of Portland Contact:

Captain John Brooks

Portland Police Bureau

1111 SW 2nd Avenue

Portland, OR 97204

TEL: 503-266-1104

TEL: (503) 823 - 0000

E-MAIL: smithb@canbypolice.com

E-MAIL: john.brooks@portlandoregon.gov

RECITALS

WHEREAS, the City has acquired a law enforcement Records Management System (“System”) to maintain a multi-agency, multi-jurisdictional set of law enforcement applications and associated databases; and

WHEREAS, the City and the RPA are both signatories to the Intergovernmental Agreement for the User Board of the Regional Justice Information Network (RegJIN); and

WHEREAS, the RPA is an Entry RPA as defined in the Intergovernmental Agreement for the User Board of the RegJIN and herein; and

WHEREAS, the RPA desires to fully use the System; and

WHEREAS, the City and the RPA desire to enter into this Agreement and being fully advised; and

NOW THEREFORE, IN CONSIDERATION of the mutual promises and covenants contained herein, it is agreed as follows:

1. DEFINITIONS:

The following is a definition of terms used herein:

- A. "Access" means the authority granted by the City to the RPA's Authorized Users to review or receive information from the System.
- B. "Agreement" means this Participating Intergovernmental Agreement and all the Terms and Conditions, including all the documents referenced in the Order of Precedence.
- C. "Amendment" means a written document required to be signed by both Parties when in any way altering the Terms and Conditions or provisions of the Agreement.
- D. "Authorized Use" means functions and capabilities that a User is assigned and able to perform based on User ID and Password, as established by a System Administrator.
- E. "Authorized System User" means any User that has passed the authentication process of the System and is thereby authorized to Use the System's functions and components based on the permissions established by that User's credentials (User ID and password, fingerprints, etc.).
- F. "City Confidential Information" means any information, in any form or media, including verbal discussions, whether or not marked or identified by the City, which is reasonably described by one or more of the following categories of information: (1) financial, statistical, personnel, human resources data or Personally Identifiable Information as described in the Oregon Consumer Identity Theft Protection Act of 2007; (2) business plans, negotiations, or strategies; (3) unannounced pending or future products, services, designs, projects or internal public relations information; (4) trade secrets, as such term is defined by ORS 192.501(2) and the Uniform Trade Secrets Act ORS 646.461 to 646.475; (5) Exempt per ORS 192.501 and/or ORS 192.502 (6) attorney/client privileged communications, (7) exempt per federal laws (including but not limited to Copyright, HIPAA) and (8) information relating to or embodied by designs, plans, configurations, specifications, programs, or systems developed for the benefit of the City including without limitation, data and information systems, any software code and related materials licensed or provided to the City by third parties; processes; applications; codes, modifications and enhancements thereto; and any work products produced for the City.
- G. "Confidential Information" means any information that is disclosed in written, graphic, verbal, or machine-recognizable form, and is marked, designated, labeled or identified at the time of disclosure as being confidential or its equivalent; or if the information is in verbal form, it is identified as confidential or proprietary at the time of disclosure and is confirmed in writing within thirty (30) days of the disclosure. Confidential Information does not include any information that: is or becomes publicly known through no wrongful or negligent act of the receiving party; is already known to the receiving party without restriction when it is disclosed; is, or subsequently becomes, rightfully and without breach of this Contract or any other agreement between the Parties or of any applicable protective or similar order, in the receiving party's possession without any obligation restricting disclosure; is independently developed by the receiving party without breach of this Contract; or is explicitly approved for release by written authorization of the disclosing party.

- H. "Cost Allocation Formula" means the Plan, adopted by the City based on recommendations by the User Board that apportions capital, operation, maintenance, repair and equipment replacement costs and use of grant funding among the Entry RPAs and Inquiry Only RPAs. The Cost Allocation Formula may be amended as provided for in the User Board Master IGA.
- I. "Criminal History Record Information" means information collected by criminal justice agencies and stored or available through the System on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any dispositions arising therefrom, including, but not limited to sentencing, correctional supervision, and release.
- J. "Criminal Justice Information" means information collected by criminal justice agencies that is needed for their legally authorized and required functions. This includes Criminal History Record Information and investigative and intelligence information. It does not include agency personnel or administrative records used for agency operations or management.
- K. "Days" shall mean calendar days, including weekdays, weekends and holidays, beginning at midnight and ending at midnight twenty-four hours later, unless otherwise specified by the Agreement.
- L. Defects means one of the five types of Defects listed below and as outlined in Exhibit E, Defect Definitions and Versaterm Responses:
- 1) "Material Defect" means an Error that impairs the Products as described in Critical Defect and for which no fix is available or forthcoming.
 - 2) "Critical Defect" means an Error as defined in the System maintenance and support agreement between the City and the System Contractor and at least 25% of the User base of the Production System are impacted in the same manner as defined in the System maintenance and support agreement for a Critical Defect.
 - 3) "High Defect" means an Error as defined in the System maintenance and support agreement between the City and the System Contractor and at least 25% of the active User base of the Production System and/or Hot Standby System environment are impacted in the same manner as defined in the System maintenance and support agreement for a High Defect.
 - 4) "Medium Defect" means an Error as defined in the System maintenance and support agreement between the City and the System Contractor.
 - 5) "Low Defect" means a Defect as defined in the System maintenance and support agreement between the City and the System Contractor. "Dissemination (Disseminate)" means the transmission of information, whether in writing, or electronically, to anyone outside the RPA that maintains the information, except reports to an authorized repository.
- M. "Documentation" means User manuals, and other written and electronic materials in any form that describe the features or functions of the System, including but not limited to

published specifications, technical manuals, training manuals, and operating instructions.

- N. "Entry RPA" means a law enforcement agency that has signed the User Board IGA and this Participant IGA with the City. Entry RPA, the City and their Authorized Users enter data into the System.
- O. "Equipment" means any hardware, machinery, device, tool, computer, computer components, computer system or other high-technology equipment, including add-ons, or peripherals of tangible form together with the necessary supplies for upkeep and maintenance, and other apparatus necessary for the proper execution, installation and acceptable completion of the System.
- P. "Error" means any defect, problem, condition, bug, or other partial or complete inability of the System to operate in accordance with the applicable Specifications and Documentation.
- Q. "Interface" means a point of interaction between System components or the device or code which enables such interaction; applicable to both Equipment and Software.
- R. "Inquiry Only RPA" means a law enforcement agency that has signed a Participant IGA with the City, providing Access to view System data but does not input any agency data into the System.
- S. "Intelligence and Investigative Information" means information compiled in an effort to anticipate, prevent, or monitor possible criminal activity, or compiled in a course of investigation of known or suspected crimes.
- T. "Material Breach" means any breach of this Contract that (a) causes or may cause substantial harm to the non-breaching party; or (b) substantially deprives the non-breaching party of the benefit it reasonably expected under this Contract.
- U. "Mobile Data Computer (MDC)" means commercial grade mobile computers operating in a law enforcement vehicle or otherwise not connected via a local or wide area network that are capable of Accessing System servers via a network connection that is compliant with the Federal Bureau of Investigation's Criminal Justice Information System (CJIS) security policies.
- V. "Operation and Maintenance Cost" shall mean the budgeted amount required for the operation, maintenance, and support of the System which may include, but not be limited to, the direct cost for: license fees, vendor support costs, software and hardware upgrade and/or replacement costs, administrative support of the User Board, maintenance, personnel, direct costs, facilities use and rental costs, and training for the upcoming year.
- W. "Personal Computer (PC)" means commercial grade desk top computers that are capable of accessing System servers via a CJIS compliant connection.
- X. "Person" means an individual of any age, concerning whom Criminal History Record Information is contained in, or accessible through the System.
- Y. "RPA Asset" shall mean hardware, software, equipment, real property and fixtures, owned or leased by the RPA.

- Z. "Specifications" shall mean the specifications contained in the contract between the City and the Contractor for the System governing its implementation and use by the City, Entry RPA, and Inquiry Only RPA.
- AA. "System" is the law enforcement records management system acquired and implemented by the City of Portland for use by the Portland Police Bureau and the RPA.
- BB. "System Administrator" shall mean a specially trained Authorized User that is authorized to perform System administrative functions.
- CC. "System Manager" is the individual with designated named backups appointed by the City of Portland to manage and operate the System on a daily basis.
- DD. "Use" means the City authorized Access given to RPA to assign Users, permission levels, enter data, and receive information from the System.
- EE. "User" shall mean any person employed by or working on behalf of the City or an RPA, the City's and RPA's Bureaus and Divisions, Officers, Directors, and any person or entity authorized by the City and/or RPA to provide it with Services requiring use of the System, and to use the City's or an RPA's resources in whole or in part, in the course of assisting the City or an RPA.
- FF. "User Board" shall mean the advisory body for the System that operates under the Master Intergovernmental Agreement for the User Board of the Regional Justice Information System Network (RegJIN).
- GG. "User Fees" are fees set by the City for RPA Access and use of the System and as agreed to between the City and a RPA in a Participating IGA. User Fees shall be updated annually based on the Cost Allocation Formula and do not require an Amendment.
- HH. "Withdrawal Plan" is a plan outlined in the User Board Master IGA, providing the manner of complete withdrawal of the RPA from this Agreement or for the RPA to change to an Inquiry Only RPA.

2. ORDER OF PRECEDENCE:

In the event there is a conflict between the terms and conditions of one portion of this Agreement with another portion of this Agreement, the conflict will be resolved by designating which portion of the Agreement documents takes precedence over the other for purposes of interpretation, except where a clear statement of precedence other than that set forth in this section is included in the document. In this Agreement the order of precedence shall be:

Exhibit A – User Fees (Fiscal Year 2014-2015)

Exhibit B – Use Policy for LInX Northwest

Exhibit C – System Procedures and Use Policy*

Exhibit D – Equipment and Security Requirements*

Exhibit E – Exhibit E, Defect Definitions and Versaterm Responses

*Exhibits C and D are available on the System's website at:

<http://www.portlandonline.com/regjinrc/index.cfm?&c=51409>. Exhibits C and D will be revised as necessary to conform to updated requirements and procedures.

3. STATEMENT OF PURPOSE:

The purpose of this Agreement is to define the terms and conditions under which the System will be Accessed and Used by the RPA.

4. SYSTEM ACCESS:

The City will contract with the System Contractor and will own all licenses to Access the System. The City will provide the RPA's Users Access to the System.

5. PROVIDED SERVICES:

- A. Enable Access via Equipment, including PCs, MDC, and other hand held devices for Authorized Use of the System by RPA Users.
- B. Provide the capability through the System to generate Oregon National Incident Reporting System (O-NIBRS) data for the RPA and to upload the O-NIBRS data to the State of Oregon in the proper format.
- C. Provide procedures, instructions and other documents to the RPA regarding the methods available and minimum requirements for RPA PCs and MDCs to gain Access to the System.
- D. Provide instructions, documents, and arrange for the necessary training to certify one or more RPA System Administrators to perform limited administrative functions such as adding and removing Users from the System, establishing User IDs and passwords, setting up each User's Authorized Uses, and resetting passwords. RPA System Administrators will be trained as required, but not more than five (5) RPA employees will be trained at any one time.
- E. Support the RPA's System Administrators in the performance of their System related administrative functions.
- F. Provide training materials, training mentors and access to the System's training environment to enable RPA trainers to provide System training and instruction to RPA Users.
- G. Maintain and administer the System according to City of Portland Information Technology policies and procedures including backup and restore, operating system patches, and System version upgrades as required and certified by the System Contractor.
- H. Monitor, audit, and trouble-shoot the upload of appropriate information from the System to the Oregon Law Enforcement Data System (LEDS), NCIC, and other interfaced crime and public safety databases and systems including but not limited to LinX Northwest.
- I. Ensure that audit logs are maintained in the System in accordance with CJIS requirements.
- J. Provide trouble reporting, trouble diagnostics and phone support on a 24-hour, 365 days

per year basis.

- K. Acknowledge trouble report calls within 30 minutes of receipt.
- L. Initiate Critical Defect or High Defect resolution supports within 2 hours or as specified within Exhibit E. Verified System Critical and High Defect Errors will be resolved as specified in the City's System's maintenance and support agreement with the System Contractor and as outlined in Exhibit E.
- M. Initiate Medium Defect and Low Defect Error resolution Monday thru Fridays from 0800-1700, excluding recognized City of Portland Holidays.

6. RPA RESPONSIBILITY:

- A. Compliance with Applicable Law. RPA warrants it has complied and shall comply with all applicable law, ordinances, orders, decrees, labor standards and regulations of its domicile and wherever performance occurs in connection with the execution, delivery, and performance of this Agreement.
- B. The RPA acknowledges and agrees that RPA employees will only use the System for Authorized Uses. Permission to use the information available in or through the System other than for Authorized Use shall be obtained in writing from the City prior to any such use.
- C. The RPA acknowledges and agrees that RPA employees and subcontractors will only Access the System and information available in or through the System as authorized in this Agreement. Permission to Access the System or information available in or through the System other than as authorized in this Agreement shall be obtained in writing from the City prior to any such Access.
- D. The RPA acknowledges and agrees that the RPA, RPA employees, and RPA subcontractors will not modify through computer programming or other techniques the functions, capabilities, and operations of the System unless written authorization is provided by the System Manager prior to performing such modifications.
- E. The RPA acknowledges and agrees that; pursuant to the directions of the Oregon State Police and Part IV of the National Crime Information Center (NCIC) Computerized Criminal History, Program Concepts and Policy; the City shall establish policy and exercise management control over all operations of the System. The System Procedures and Use Policy is attached as Exhibit C.
- F. RPA Administrators shall be responsible for creating User IDs, passwords, and establishing the Authorized Uses of the System for RPA Users within the constraints of the policies and procedures established by the City for such Users.
- G. RPA is responsible for providing its own Equipment, including PCs, MDCs, printers, and other RPA located devices required by RPA Users of the System.
- H. The RPA acknowledges and agrees that all RPA Equipment such as PCs and MDCs with Access to the System will be configured to meet the System's minimum requirements to gain Access as specified in Exhibit D: Equipment and Security Requirements.

- I. The RPA acknowledges and agrees that all RPA Users shall meet the Personnel Security requirements specified in Exhibit D: Equipment and Security Requirements.
- J. RPA is responsible for maintaining RPA PCs and MDCs according to City established requirements as specified in Exhibit D: Equipment and Security Requirements for the System.
- K. RPA is responsible for installing, configuring and providing network access to devices located in RPA facilities and vehicles including, but not limited to, printers, scanners, and image capture devices.
- L. RPA is responsible for providing secure network Access that 1) meets CJIS security requirements and 2) enables RPA PCs to reach the System's network demarcation points.
- M. RPA is responsible for providing network connectivity that meets CJIS security policies and for providing all network communication devices and Equipment between RPA MDCs and the System.
- N. RPA is responsible for ensuring that all RPA network infrastructure and workstations with Access to the System comply with the most current CJIS security policy including, but not limited to, the physical security of workstations and MDCs that are able to Access the System, access control, identification and authentication, information flow enforcement, and system and information integrity. RPA may contact the City to determine how to obtain the most current version of the CJIS security policy document. The RPA is responsible for curing any problems uncovered as a result of an FBI audit. The City reserves the right to request and receive within a reasonable period, verification of RPA's compliance with CJIS policies.
- O. RPA is responsible for correcting any O-NIBRS data identified by the System or by the State.
- P. RPA is responsible for providing the City with the most current contact information for the RPA's security personnel and any changes thereof within seven (7) days of the change.
- Q. RPA is responsible for ensuring that all RPA Users that are granted Authorized Use of the System comply with the appropriate CJIS security requirements.
- R. RPA is responsible for checking the accuracy of, and generating standard O-NIBRS data for RPA and for the upload of the O-NIBRS information to the State of Oregon through the System.
- S. RPA acknowledges and agrees that data entered into the System by RPA Users shall conform to the standards and procedures established for the System as described in Exhibit C, System Procedures and Use Policy. The City shall notify the RPA in writing if data entered by RPA Users is found to be nonconforming to the established standards and procedures. The RPA shall, at its option, 1) Correct such data using RPA resources as soon as practicable, but not to exceed thirty (30) days, or 2) request assistance by the City and reimburse the City for any costs associated with the City's removing or performing remedial actions on RPA data required to bring the data into conformance with established standards and procedures.

7. LInX NORTHWEST:

- A. The RPA acknowledges and agrees to abide by all use policies set forth for participation in the NCIS Law Enforcement Information Exchange (LInX Northwest) system as stipulated in Exhibit B: Use Policy for LInX Northwest.
- B. The RPA authorizes the City to provide the RPA's public records category data that is contained in the RegJIN RMS to LInX Northwest for Access and authorized Use by LInX Northwest users.

8. CONFIDENTIALITY:

- A. Maintenance of Confidentiality. The City and RPA shall treat as confidential any Confidential information that has been made known or available to them or that an Entry RPA has received, learned, heard or observed; or to which an RPA has had access. The City and RPA shall use Confidential information exclusively for the City or RPA's benefit and in furtherance of this Agreement. Except as may be expressly authorized in writing by the City or RPA, in no event shall the City or RPA publish, use, discuss or cause or permit to be disclosed to any other person such Confidential information. The City and RPA shall (1) limit disclosure of the Confidential information to those directors, officers, employees and agents of the City or RPA who need to know the Confidential information, (2) exercise reasonable care with respect to the Confidential Information, at least to the same degree of care as the City or RPA employs with respect to protecting its own proprietary and confidential information, and (3) return immediately to the City or RPA who provided the information, upon its request, all materials containing Confidential Information in whatever form, that are in the City or RPA's possession or custody or under its control. The City and RPA are expressly restricted from and shall not use Confidential intellectual property of the City or providing RPA without the City or that RPA's prior written consent.
- B. The RPA acknowledge that each RPA is subject to the Oregon or Washington Public Records Acts, as applicable, and Federal law. Third persons may claim that the Confidential Information may be, by virtue of its possession by the City or a RPA, a public record and subject to disclosure. RPA receiving a public records request agrees, consistent with its state public records law, not to disclose any information that includes a written request for confidentiality and as described above and specifically identifies the information to be treated as Confidential. A RPA's commitments to maintain information confidential under this Agreement are all subject to the constraints of Oregon or Washington Statutes and Federal laws. Within the limits and discretion allowed by those laws, the City and RPA will maintain the confidentiality of information.
- C. The RPA acknowledge and agree that the City and each RPA owns its own data in the System. RMS data can only be disclosed by the agency that entered it. In the event of a public record request for System data which belongs to the City or another RPA, the City or receiving RPA shall inform both the requestor and the appropriate RPA within two business days that it is not the custodian of record for the requested data and identify the RPA that may be able to comply with the public record request.
- D. The RPA acknowledge that unauthorized disclosure of Confidential Information will result in irreparable harm to the City or providing RPA. In the event of a breach or threatened breach of this Agreement, the City or affected RPA may obtain equitable relief prohibiting the breach, in addition to any other appropriate legal or equitable relief.

9. LIMITS ON DISSEMINATION:

The RPA's Dissemination of Criminal Justice Information available in or through the RegJIN RMS shall follow current Criminal Justice Information policies and procedures and/or other applicable State and/or Federal Laws.

10. INFORMATION CONTROL AND RESPONSIBILITY:

Additions, modifications, and deletions of information stored in the RegJIN RMS shall be restricted to specifically authorized RPA Users and devices. The City will provide the RPA with a list of RPA sworn personnel, Users and devices that are permitted Access to the System on an annual basis. The RPA shall verify the list and report any discrepancies within 60 days. The responsible Party shall update the list of authorized Users and devices in a timely manner.

11. EQUITABLE REMEDIES:

The RPA acknowledges that unauthorized disclosure of City Confidential Information or misuse of a City computer system or network will result in irreparable harm to the City. In the event of a breach or threatened breach of this Contract, the City may obtain equitable relief prohibiting the breach, in addition to any other appropriate legal or equitable relief.

12. SECURITY:

- A. Physical Security – the RPA shall be responsible for maintaining the physical security of all devices that are authorized to Access the System, as well as any printed output or System Documentation which might permit unauthorized Access to, or use of the System from within the RPA.
- B. On-Line Security – The System contains procedures and tools to ensure that only authorized RPA Users and RPA devices can Access the information available in or through the System. RPA Users will be required to enter System User IDs and passwords before gaining Access to the System. System functions and System data. The RPA is responsible for issuing individual System User IDs and passwords to RPA Users. The RPA acknowledges and agrees that RPA employees will not share System User IDs and passwords.
- C. Personnel Security – Any individuals that are provided Access to the System by the RPA through the issuing of System IDs and passwords shall undergo the following security checks:
 - 1) A personal background investigation equivalent to a background investigation that would enable them to access the RPA's own confidential information.
 - 2) Be fingerprinted and their identification and personal history verified through a check of the System's master name index, Oregon LEADS, the National Crime Information Center, and the FBI's Criminal Identification files.
 - 3) Obtain appropriate certifications from the Oregon State Police for any LEADS and NCIC transactions for which the User is authorized to perform within the System.
- D. The RPA acknowledges and agrees to comply with applicable CJIS Security Policy, including, but not limited to, verifying identification, performing a state of residency and

national fingerprint-based record check within 30 days of assignment for all personnel who have direct access to Criminal Justice Information through RegJIN and for those RPA employees or contractors who have direct responsibility to configure and maintain computer systems and networks with direct access to Criminal Justice Information through RegJIN. If applicable, RPA shall deny or terminate Access and deny issuing or revoke a System User ID and password if, upon investigation, any RPA employee requesting or currently Using a System User ID and password is found to be in violation of current CJIS policy.

- E. The RPA acknowledges and agrees to immediately deactivate the System USER ID and password of any employee or contractor who is no longer an RPA employee, an RPA contractor, or who no longer requires Access to the System.
- F. RPA shall provide immediate notification to the System Manager of any security breach that affects the System or any other City systems. RPA shall provide notification to the System Manager of any incident relating to System integrity such as a computer virus.
- G. Failure to comply with the Security and Access specifications contained in the Agreement and Exhibit D: Equipment and Security Requirements may, at the sole discretion of the City, result in the suspension of the RPA and the RPA Users' Access to the System until such failures are corrected to the City's satisfaction.

13. PROPRIETARY RIGHTS:

All trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to each Party are and will remain the exclusive property of that Party.

14. PAYMENT:

- A. RPA acknowledges and agrees to pay the City the amount set out in Exhibit A: User Fees, which shall conform to the Entry RPA cost allocations contained in the Cost Allocation Formula in the User Board Master IGA in effect at the time of billing.
- B. Additional RegJIN services and/or System functions that are not routinely provided to other Entry RPAs under this Agreement shall be added via Amendment and billed as a separate line item identified in Exhibit A.
- C. Exhibit A, User Fees, shall be adjusted to conform to changes in the Cost Allocation Formula or in the services and/or System functions provided by the City to the RPA.
- D. The City will invoice the RPA annually in conformance with Exhibit A: User Fees.
- E. The RPA shall submit payment within thirty (30) days of receipt of the invoice from the City.
- F. Failure to pay the City as due will suspend the RPA's Access to the System until fully paid up.
- G. In order to conform to the Cost Allocation Formula in the User Board Master IGA and to enable the invoice preparation per Exhibit A, RPA shall provide the City with the RPA's number of authorized sworn personnel plus any correctional deputies that will Access the System by April 1 of the calendar year before the next fiscal year during which the

invoices apply.

15. CITY AUDITS:

The City, either directly or through a designated representative, may conduct financial and performance audits. City audits shall be conducted in accordance with generally accepted auditing standards. RPA shall provide the City's internal auditor or external auditor, and their designees with a copy of all reports, including any management letters issued as a result of the specified audits.

Access to Records – The City internal auditor or City external auditor, and their designees, shall be given the right, and the necessary access, to review the work papers of RPA audits if the City deems it necessary. Copies of applicable records shall be made available upon request at no cost to the City.

16. DURATION, WITHDRAWAL AND TERMINATION:

- A. This Agreement is perpetual and shall continue from year to year unless otherwise terminated.
- B. This Agreement may be terminated by either Party by the provision of a 90-Day written notice of termination to the other Party. Termination notices must be provided in writing and sent by either certified US mail, return receipt requested, or by personal delivery.
- C. The effective date of termination shall be on January 1 of the year following the year during which the 90-day written notice expired.
- D. Upon the effective date of termination, the RPA may remove its RPA assets from the System including any System data belonging to the RPA. All costs associated with the reasonable removal of the RPA's assets including System data owned by the RPA will be the responsibility of the RPA, unless termination notice is provided by the City in which case the City will either keep the data or the RPA will be responsible for all costs associated with the reasonable removal of the RPA's assets including System data owned by the RPA.
- E. A minimum of 180 days shall be allocated for the System Manager to withdraw an RPA's assets including System data owned by the RPA from the System after the date upon which the termination becomes effective. The RPA may, at its option, continue to Access the System during this period.
- F. In the event of termination, RPA shall pay the City for work performed in accordance with the Agreement prior to the effective date of termination.

17. FORCE MAJEURE:

- A. In the event that either Party is unable to perform any of its obligations under this Agreement (or in the event of loss of Use) due to natural disaster, actions or decrees of governmental bodies or communications line failure not the fault of the affected Party (hereinafter referred to as a "Force Majeure Event"), the Party who has been so affected immediately shall give notice to the other Party and shall do everything possible to resume performance.

- B. If the period of nonperformance exceeds fifteen (15) Calendar Days from the receipt of notice of the Force Majeure Event, the Party whose ability to perform has not been so affected may, by giving written notice, terminate this Agreement.

18. VIOLATIONS OF THE AGREEMENT:

In the event of violation of the provisions of this Agreement, or violation of the security policy by the RPA, RPA employees, and/or RPA contractors, the City shall have the authority to immediately restrict or prohibit Access to the System by RPA Users, RPA PCs, RPA MDCs, and other RPA devices until resolution of the problem to the satisfaction of the City. The RPA shall be notified in writing of such action, given 30 days in which to cure the violation before Access is restricted or prohibited, and there shall be no charge for Access during any time that Access is prohibited.

19: ROLLING ESTOPPEL:

Unless otherwise notified by the RPA, it shall be understood that the City shall have met all its obligations under the Agreement. The City will be conclusively deemed to have fulfilled its obligations, unless it receives a deficiency report from the RPA within ninety (90) Days of the alleged deficiency and the RPA identifies the specific deficiency in the City's fulfillment of its obligations in that report. Deficiencies must be described in terms of how they have affected a specific performance requirement of City.

20. DISPUTE RESOLUTION:

The RPA shall cooperate with the City to assure that all claims and controversies which arise under this Agreement and which might affect the quality of such Services will be resolved as expeditiously as possible in accordance with the following resolution procedure:

- A. Any dispute between the City and RPA under this Agreement shall be resolved, if possible by the System Manager or their designee on behalf of the City and Bret Smith or City of Canby designee on behalf of the RPA.
- B. If the System Manager or the System Manager's designee and RPA are unable to resolve any dispute within three (3) Business Days, or such other time as mutually agreed upon, after notice of such dispute is given by either Party to the other, the matter shall be submitted to Bureau of Technology Services Chief Technology Officer on behalf of the City and Information Services Director and Bret Smith or City of Canby designee on behalf of the RPA for resolution, if possible.
- C. If the City's Chief Technology Officer and the RPA's Bret Smith or City of Canby designee RPA's are unable to resolve any dispute within fourteen (14) Calendar Days, or such other time as mutually agreed upon, the dispute shall be escalated to the Chief of Police/Sheriff.
- D. Should any dispute arise between the Parties concerning this Agreement that is not resolved by mutual agreement above within thirty (30) Calendar Days, or such other time as mutually agreed upon, it is agreed that such dispute will be submitted to mandatory mediated negotiation prior to any Party's commencing binding arbitration or litigation. In such an event, the Parties to this Agreement agree to participate in good faith in a non-binding mediation process. The mediator shall be selected by mutual agreement of the

Parties, but in the absence of such agreement each Party shall select a temporary mediator and those mediators shall jointly select the permanent mediator. All costs of mediation shall be borne equally by the Parties.

- E. Should an equitable solution not result from the foregoing, the City and Contractor shall be free to agree to pursue either binding arbitration, litigation, or other remedies allowed under this Agreement.
- F. In the event the Parties elect to use arbitration to settle the dispute, within thirty (30) Days of a notice by either Party to the other requesting arbitration, the affected RPA shall select an arbitrator from a list of three (3) obtained from Arbitration Services of Portland, Inc. (ASP). For the avoidance of doubt, issues related to technology require an arbitrator with a background in computer systems or technology. The arbitrator shall, for purposes of the arbitration proceedings, apply the rules of mandatory arbitration as adopted by the ASP in effect at the time of the arbitration. Within sixty (60) Days of the appointment of the arbitrator, the Parties shall concurrently submit to the arbitrator (supplying a copy to each other) a written statement of their respective legal and factual positions on the dispute. The arbitrator shall determine, after a hearing on the merits and within forty-five (45) Days after receipt of the statements, the determination of the dispute which determination shall be final and binding. Each Party shall bear equally the expense of the arbitrator and all other expenses of conducting the arbitration. Each Party shall bear its own expenses for witnesses, depositions, other costs incurred and attorney's fees.
- G. Unless ordered by the City to suspend Access, the RPA shall proceed with Use without any interruption or delay during the pendency of any of the foregoing dispute resolution. During the pendency of any of the foregoing dispute resolution procedures, the RPA shall continue to make all payments that are not in dispute, in accordance with the provisions of the Agreement.

21. NOTICE:

Any notice provided for under this Agreement shall be sufficient if in writing and delivered personally to the following address or deposited in the United States Mail, postage prepaid, certified mail, return receipt requested, addressed as follows, or to such other address as the receiving Party hereafter shall specify in writing:

If to the Provider:

RegJIN System Manager
Portland Police Bureau
1111 SW Second Avenue, Room 1156
Portland, Oregon 97204-3232

If to the RPA:

Agency Contact Info
Bret Smith
Chief of Police
Canby Police Department
1175 NW 3rd Avenue
Canby, OR 97013

22. AMENDMENTS:

Except as a section or subsection may otherwise specifically provide, limit, or prohibit, the City and RPA may amend this Agreement at any time only by written Amendment executed by the City and the RPA.

Any changes to the provisions of this Agreement shall be in the form of an Amendment. No provision of this Agreement may be amended unless such Amendment is approved as to form by the City Attorney and executed in writing by authorized representatives of the Parties. If the requirements for Amendment of this Agreement as described in this section are not satisfied in full, then such Amendments automatically will be deemed null, void, invalid, non-binding, and of no legal force or effect.

23. INTERPRETATION:

The terms and conditions of this Agreement shall be liberally construed in accordance with the general purposes of this Agreement and according to Oregon law. This Agreement shall be construed according to the laws of the State of Oregon without reference to its conflict of law provisions. Any litigation between the City and RPA arising under this Agreement shall occur, if in the state courts, in the Multnomah County Circuit Court, and if in the federal courts, in the United States District Court for the District of Oregon.

24. INDEMNIFICATION:

To the extent permitted by the Constitutions and laws of Oregon the RPA and the City shall hold each other harmless and indemnify each other for the negligent acts, actions or omissions to act of their respective entity's, commissioners, officers, employees, and agents in the performance of their respective responsibilities and duties under this Agreement. Notwithstanding the foregoing, neither Party shall in any way be liable to hold harmless or indemnify the other Party for any costs or claims arising directly, or indirectly, out of any System related activities in which they are not participating.

25. ASSIGNMENT:

The rights and obligations of each party under this Agreement may not be assigned in whole or in part. Any attempted transfer shall be null and void, of no force or effect. Attempted transfer of this Agreement shall be considered Material Breach of contract.

26. WAIVER:

No waiver or any breach of Agreement shall be held to be a waiver of any other or subsequent breach of this Agreement.

27. REMEDIES:

The remedies provided in this Agreement are cumulative, and may be exercised concurrently or separately. The exercise of any one remedy shall not constitute an election of one remedy to the exclusion of any other.

28. SURVIVAL:

All obligations relating to confidentiality; indemnification; publicity; representations and

warranties; proprietary rights as stated in this Agreement shall survive the termination or expiration of this Agreement.

29. NO THIRD PARTY BENEFICIARIES:

The Parties expressly agreed that nothing contained in the Agreement shall create any legal right or inure to the benefit of any third party.

This Agreement is entered into for the benefit of the City and RPA. Except as set forth herein, nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for breach of contract, personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

30. SEVERABILITY:

The terms of this Agreement are severable and a determination by an appropriate body having jurisdiction over the subject matter of this Agreement that results in the invalidity of any part, shall not affect the remainder of this Agreement.

31. INTEGRATION:

This Agreement and the User Board IGA contains the entire Agreement between RPA and the City and supersedes all prior written or oral discussions or agreements.

The City: City of Portland	RPA: City of Canby
By:	By:
Name: Mike Reese	Name: Bret Smith
Title: Chief of Police	Title: Chief of Police
Date:	Date:
By:	By:
Name: Kalei Taylor	Name: Joseph Lindsay
Title: City Attorney for the City of Portland	Title: City Attorney – City of Canby
Date:	Date:

Exhibit A: User Fees
Fiscal Year – July 1, 2015 to June 30, 2016

RPA agrees to pay the City of Portland the following annual User Fees for System Access and Use. RPA shall be billed yearly. Partial year amounts shall be pro-rated. The User Fees conform to the Entry RPA cost allocations contained in the Cost Allocation Formula in the Master User Board IGA in effect at the time of billing.

Sustainment Budget.....	\$ 2,106,188
Total Number of RegJIN Users	2,901
Cost Per User per month.....	\$ 61.00
Total Number of RegJIN Users from Canby Police	25

Annual Cost for RegJIN Access and Use for the Canby Police	\$18,300
---	-----------------

Exhibit B: Use Policy for LInX Northwest

Fiscal Year – July 1, 2014 to June 30, 2015

The Law Enforcement Information Exchange (LInX Northwest) is a law enforcement information sharing partnership involving local, state, and federal law enforcement agencies in the Northwest. LInX has been developed to improve public safety, solve crime, and prevent terrorism. LInX is a partnership built on trust and to maintain that trust the following rules are upheld by all LInX agencies. Violations of this policy may result in sanctions against an individual User or his/her Regional Partner Agency.

1. Each Regional Partner Agency shall contribute information to LInX Northwest, once a connection is made, and agrees to permit the Access, dissemination, and/or Use of such information by every other partner agency in LInX Northwest. The contributing party has the sole responsibility and accountability for ensuring that it is not constrained from permitting this by any laws, regulations, policies, and procedures applicable to the submitting party.
2. A user may only access LInX when he/she has a legitimate, official law enforcement purpose, after receiving LInX training.
3. Information in the system shall not be disseminated outside of an accessing party without first obtaining express permission of each party that contributed the information in question. LInX users who wish to use information in LInX for the preparation of judicial process such as affidavits, warrants, subpoenas, etc... agree to not print and use information from LInX, but to contact the originating agency who will FAX or email a copy of the original report to the requestor for court or other official uses.
4. Printing copies from LInX is highly restricted. Users may only retain printed copies temporarily and shall not place printed copies in an official file or submit them to a court. Printed copies must be destroyed, shredded, or burned promptly. Printed copies may not be made for members of non-participating agencies.
5. Any requests for reports or data in LInX records from anyone other than a party to this Exhibit will be directed to the contributing party. Participating agencies in LInX agree to not disclose another agency's reports or information to a third party. Even when an agency receives an official request for disclosure, LInX agencies agree to refer such requests to the originating agency of the report for action.
6. Each Agency retains sole ownership of, sole responsibility for, and exclusive control over the content of the information that it contributes to LInX, and it may, at will, at any time update, correct, or delete the information that it contributes to LInX.
7. Regional Partner Agencies will have access to LInX via a secure Internet connection. RPA are responsible for providing and maintaining their own Internet connectivity to LInX.
8. LInX will maintain an audit capability that will log the date, time, subject, and originating account of all user queries. The LInX Governance Board will maintain these audit logs for at least five years.

Exhibit C: System Procedures and Use Policy:
Fiscal Year – July 1, 2015 to June 30, 2016

This Exhibit is currently under development and will be provided as soon as it is available. This document is a place holder for the exhibit.

Exhibit D: Equipment and Security Requirements:
Fiscal Year – July 1, 2015 to June 30, 2016

Workstation Type	Application	Manufacturer	Specifications
Versadex Desktop	RMS	HP / Dell / IBM or equivalent	<ul style="list-style-type: none"> • Intel or AMD 2 GHz dual core processor • Memory <ul style="list-style-type: none"> ○ 2 GB (minimum) ○ 4 GB (recommended) • 20 GB (available) HDD • NIC <ul style="list-style-type: none"> ○ 10 Mbit minimum ○ 100 Mbit recommended • 1024x768+ resolution display monitor • Microsoft Windows XP, Vista or 7
Versadex Mobile	Field Reporting	Panasonic, Motorola or equivalent	<ul style="list-style-type: none"> • Intel Centrino dual core processor • 2GB RAM • Display Resolution <ul style="list-style-type: none"> ○ 800x600 minimum ○ 1024x768 recommended • 13.3" daylight-readable LCD with (preferable) touchscreen • 20 GB (available) HDD • Microsoft Windows XP, Vista or 7

1. **Access Security** - New, desktop and mobile Equipment with access to the PPDS System must adhere to the following requirements:
 - 1.1. Both desktop and mobile Equipment shall employ virus protection software
 - 1.1.1. Use of Anti-Virus and Anti-Spyware software to scan, detect, and eliminate viruses on workstations and laptops
 - 1.1.2. Anti-Virus and Anti-Spyware software must be kept up to date with current virus definitions, run at start-up, and employ resident scanning
 - 1.2. Both desktop and mobile Equipment shall apply current operating system service packs and patches; Auto-update is recommended.
 - 1.3. All desktop and mobile Equipment shall be protected by a current firewall.
 - 1.4. All mobile Equipment shall employ encryption technology for wireless transmissions from origin to termination. Encryption shall comply with Federal Information Processing Standards (FIPS) publications and guidelines for encryption.
 - 1.5. All mobile Equipment shall employ virtual private network for those transmissions that traverse between wireless local area network and department trusted network segments and shall have a static private IP address.

- 1.6. All Users shall employ an auto-lock on their workstation or laptop that meets CJIS requirements.
- 1.7. The secured facility and all desktop and mobile Equipment shall employ at least one Advanced User Authentication method to secure access to data. This could include, but is not limited to, Biometrics, Smart Cards, or Electronic Token devices.
2. **Personnel Security** – Prior to gaining Access to the System’s criminal history record information, a person shall:
 - 2.1. Be fingerprinted and a background investigation conducted by the User’s RPA.
 - 2.2. That investigation shall include, but not be limited to, verification of information provided by the person and to public record information, including a check of the System’s master name file, Oregon LEDS or Washington ACCESS (depending on the state in which the RPA resides) and the National Crime Information Center files, and FBI Criminal Identification files.

Exhibit E - Defect Definitions and Versaterm Responses

Severity Level	Defect Definition	Versaterm Maintenance Response
Critical Defect	<ul style="list-style-type: none"> • Impacts at least 25% of the User base of the Production System. • Severely affects City and/or Partner agency operations (e.g., critical business processes are disabled). Alternatively, severely impacts business operations due to the accumulated impact on multiple Users. • Includes, but is not limited to, problems that cause continuous or near-continuous interruption of service (e.g., the system “hangs” or “crashes”), the loss of use of one or more major critical features functions or modules (including interfaces), file system corruption, and or data loss. • No stable workaround available. • May require manual mode operation. • Requires the City to telephone the Versaterm support telephone number 	<ul style="list-style-type: none"> • Versaterm shall normally respond within thirty (30) minutes. If Versaterm does not respond within thirty (30) minutes, the City may escalate the issue to the next responder as identified in the 7x24 Emergency Telephone Numbers contained in the Versaterm Customer Service Area web site. • Upon the City’s notification to Versaterm of a Critical Defect, Versaterm shall immediately provide expert personnel to resolve the problem via remote access and/or provide On-Site Emergency Support as described in Section 2.4 of this Support Agreement. All attempts shall be made to repair the Problem within 8 hours of City notification. • Versaterm shall maintain such expert support until the Defect is repaired to the satisfaction of the City or it is determined the Defect is caused by a non-Versaterm supplied component or software. • Versaterm and the City will communicate, as necessary, the status of repair.
High Defect	<ul style="list-style-type: none"> • Impacts at least 25% of the active User base of the Production System and/or Hot Standby System environment. • In Production System environment, causes a significant impact on business operations of Users Alternatively, causes a significant impact on business operations due to the accumulated impact on multiple Users. • This includes, but is not limited to Problems that cause intermittent disruption of service, the loss of use of multiple non-major critical features functions, significant performance degradation, the accumulation of enough Problems in a new version to delay Production rollout, or increased risk due to loss of redundancy, etc. • No stable workaround available. • May not require manual mode operation. • Requires the City to telephone the Versaterm support telephone number. 	<ul style="list-style-type: none"> • Versaterm shall normally respond within thirty (30) minutes. If Versaterm does not respond within thirty (30) minutes, the City may escalate the issue to the next responder as identified in the 7x24 Emergency Telephone Numbers contained in the Versaterm Customer Service Area web site. • Upon the City’s notification to Versaterm of a Critical Defect, Versaterm shall immediately provide expert personnel to resolve the problem via remote access. • Versaterm shall maintain such expert support until the Defect is repaired to the satisfaction of the City or it is determined the Defect is caused by a non-Versaterm supplied component or software. • Versaterm and the City will communicate, as necessary, the status of repair.

<p>Medium Defect</p>	<ul style="list-style-type: none"> • Impacts Production System and/or Hot Standby System environment • In Production System environment, causes a minor manageable impact on business operations of Users Alternatively, causes a minor limited impact on business operations due to the accumulated impact on multiple Users. • This includes, but is not limited to Problems that cause the loss of use of a single non-major feature, problems where a workaround exists but that measurably slows Users work performance, the existence of known minor problems in a new version scheduled for rollout, etc. • Stable workaround is available and has been successfully implemented. • The City may telephone or email Versaterm the Problem description 	<ul style="list-style-type: none"> • Versaterm shall normally respond within one (1) Business Day. • Versaterm shall provide expert support until the Defect is repaired to the satisfaction of the City or it is determined the Defect is caused by a non-Versaterm supplied component or software. • Versaterm and the City will communicate, as necessary, the status of repair.
<p>Low Defect</p>	<ul style="list-style-type: none"> • Impacts Production System environment • In Production System environment, causes little or no impact on business operations of Users. Alternatively, causes little or no impact on business operations due to the accumulated impact on multiple users. • This includes, but is not limited to problems of a cosmetic nature OR those where a workaround exists that does not have a measurable impact on task performance OR the City requires information or assistance about product capabilities or installation configuration. • The City may telephone or email Versaterm the Problem description 	<ul style="list-style-type: none"> • Versaterm shall normally respond within five (5) Business Days.