Amendment to License Agreement to Transition from On-Premise to Licensor Hosting

This amendment (herein, the "Amendment") is made to the existing Software License, Maintenance and Support Agreement (the "License Agreement"), entered into as of June 28, 2018, between Journal Technologies, Inc., a Utah corporation ("Licensor"), and Solano County on behalf of its Probation Department ("Licensee"). This Amendment is made as of the date of last signature below.

Whereas:

(a) Under the License Agreement prior to the effective date hereof, Licensor provided Licensee with User licenses to, and Maintenance and Support for the Licensed Software as defined in the License Agreement, which Licensee has hosted locally on-premise; and

(b) Licensee now desires for Licensor to provide cloud-hosting services for the Licensed Software, in accordance with the terms of this Amendment and in consideration of certain additional annual fees defined herein. For clarity: all terms updated in or introduced to the License Agreement hereby align with cloud-hosting provisions recently agreed to in a separate contract between Licensor and Licensee, on behalf of its District Attorney's Office, dated June 17, 2025.

Now, therefore, for good and valuable consideration, the sufficiency of which is acknowledged, the parties agree as follows:

1. Professional Services to Move Licensed Software to Licensor-Hosting Model.

A. To Be Accomplished Pursuant to Attached Statement of Work. The parties agree that, in accordance with the statement of work attached hereto as Attachment 1, Licensor shall accomplish the movement of Licensee's Licensed Software from a locally-hosted, on-premise setup to a cloud-hosted setup managed by Licensor, leveraging hosting infrastructure provided by Amazon Web Services (AWS).

B. SOW Governed by PSA: Pursuant to Section 2.3.2 ("Incorporations of Statement of Work") of the Professional Services Agreement (the "PSA") between the parties, executed of even date with the License Agreement, the Attachment 1 shall be governed by the terms of the PSA.

2. Incorporation of New Cloud-Hosting and Service Level Provisions as New Exhibits D and E.

A. New Exhibit D Added to License Agreement Reflecting Cloud-Hosting Services. Attached hereto as Attachment 2, a new Exhibit D ("Hosted Services") is hereby incorporated into the License Agreement. This document shall govern Licensor's provision of cloud-hosting services for the Licensed Software.

B. New Exhibit E Added to License Agreement Reflecting Service Levels. Attached hereto as Attachment 3, a new Exhibit E ("Service Level Agreement") is hereby incorporated into the License Agreement. This document details Support service levels pertaining to the Licensed Software.

3. Incorporation of New Fees for Cloud-Hosting Services into Existing Exhibit A.

A. New Section Contemplating Annual Cloud-Hosting Fees and Recurring Document Storage Fees Added to Exhibit A ("License, Maintenance and Support Fees"). The following new section is added to the License Agreement's existing pricing section (Exhibit A), reflecting the annual fee for cloud-hosting services, and the recurring fees for hosted document storage:

Annual eProbation Hosting and Storage Fees: <u>$126,250 for 325 User licenses</u> (and adjusted for any CPI increase after the first billing period). For the first period, this amount will be prorated to align with the remainder of Licensee's existing billing cycle for the License, Maintenance and Support Fees (which is July 1 to June 30). **To illustrate:** If the Licensed Software becomes live on the Licensor-provided cloud infrastructure (the "Cloud Hosting Go Live") on April 1, 2026, then Licensee will be responsible for three (3) months of the annual cloud hosting fees (i.e. $31,562.50). Then, upon July 1, the full annual fees would be assessed in combination with the then-current annual License, Maintenance and Support Fees.

Monthly Fees Prior to Cloud Hosting Go Live: In addition, for testing and quality assurance purposes, Licensee will likely leverage the Licensor-provided cloud infrastructure prior to the Cloud Hosting Go Live. Fees for such use will be charged on a monthly basis, at $10,520/month. These fees shall commence at such time as Licensor has created the AWS hosting environment for Licensee and begun to leverage it for purposes of completing the work described in this Amendment.

Document Storage. In addition to the fees above, hosted document storage shall be charged in accordance with Licensee's usage, and pursuant to the table set forth below. Document storage fees are subject to change throughout the course of the Agreement upon 60 days prior notice by Licensor:

Service	**Price per month**
Storage – Frequent Access Tier	$0.093 per GB
Storage – Infrequent Access Tier	$0.055 per GB
Storage – Archive Access Tier	$0.0278 per GB

**Storage usage is calculated in binary gigabytes (GB), where 1GB is 1,073,741,824 bytes. This unit of measurement is also known as a gibibyte (GiB), defined by the International Electrotechnical Commission (IEC)*

Licensor shall bill Licensee for Document Storage at the end of each year of the License Term; provided, however, that if Licensee's total Document Storage usage exceeds two (2) TB, Licensee will receive monthly invoices for Document Storage. The storage threshold determining the timing of Licensee payment (annually or monthly) is subject to change throughout the course of the Agreement upon 30 days' notice.

Licensee has two options for paying these fees:

Option #1: Invoice. Licensee will be sent an invoice, either annually or monthly depending on Licensee's overall Document Storage usage, for average daily storage usage. Licensee may use ACH to make its invoice payments.

Option #2: Automated. If Licensee wishes to automatically pay for their Document Storage, Licensee may set up an automatic payment plan with Licensor.

Changes in User License Count: If the number of agency Users increases or decreases, the annual Hosting and Storage Fees will be adjusted pursuant to the pricing table set forth below, but subject in all events to a minimum annual Hosting and Storage Fees of $40,000:

User Groups*	User Licenses	Annual Hosting Fees *(Excluding document storage)* Per License	For Group
1-50	50	$800	$40,000
51-100	50	500	25,000
101-200	100	300	30,000
201-500	300	250	75,000
501-1000	500	200	100,000

B. Updated Exhibit A Name. Following execution of this Amendment, the name of Exhibit A shall thereafter be "License, Maintenance, Support and Hosting and Storage Fees."

4. Certain Other Updated Terms

A. Updated "Conditions to Receive Support" Based on Change to Licensor Hosting. As of Cloud Hosting Go Live, Section 3.3.3 shall be updated as follows, to reflect that Licensee will no longer need to follow the on-premise requirements set forth in Exhibit C of the License Agreement ("Minimum System Requirements") in order to receive Support:

3.3.3 ~~Licensee must maintain all related hardware and software systems required for the operation of the Licensed Software. Minimum System requirements are attached as Exhibit C ("System Requirements").~~ Licensor shall have no responsibility for the configuring, maintaining, or upgrading Licensee's operating system, hardware network, or any other software not provided by Licensor. ~~Licensor is not responsible for creating or maintaining database or storage backup files.~~

B. Updated Grant of License Based on Change to Licensor Hosting. As of Cloud Hosting Go Live, all references to installation of the Licensed Software on Licensee systems (including, e.g., in Section 2.1, "Grant of License") shall be interpreted as a right to access and Use the Licensed Software in the cloud hosted environment provided by Licensor.

C. Update to "User" Definition. Section 1.12 is hereby updated as follows, to align with the current definition of User in Licensor's contracts, including the agreement with Solano County on behalf of its District Attorney's Office:

1.12 User means any individual person, computer terminal or computer system (including, without limitation, any workstation, pc/cpu, laptop and wireless or network node) that has been authorized by the Licensee (through a username and password) to use the Licensed Software, (b) any other non-~~court~~ **agency** government employees and contractors who are performing their jobs, or a computer terminal or computer system used by such a person, in each case, interfacing with or accessing the Licensed Software through an interface or its public portal or (c) any individual person who is a member of the general public (including litigants and their attorneys, reporters or interested citizens, but not government employees or contractors who are performing their jobs), or a computer terminal or computer system used by such a person, accessing the Licensed Software at any given time for any

reason through **an interface or** its public portal (including to file documents electronically or to view information in or accessible through the Licensed Software).

D. Update to "Certain Specific Limitations" Section Pertaining to Artificial Intelligence. Section 2.2.3 ("Certain Specific Limitations") is hereby updated as follows, to align with the current AI-related provision in Licensor's contract's generally, including in the District Attorney agreement mentioned above:

2.2.3 Certain Specific Limitations. Licensee shall not, and shall not permit any User or other party to, (a) copy or otherwise reproduce, reverse engineer or decompile all or any part of the Licensed Software, (b) make alterations to or modify the Licensed Software, (c) grant sublicenses, leases or other rights in or to the Licensed Software, ~~or~~ (d) permit any party access to the Licensed Software for purposes of programming against it, **or (e) enable, allow or cause access to the Licensed Software by any artificial intelligence or automated program not provided by or expressly authorized by Licensor.** Licensee shall be solely responsible for preventing improper, unauthorized, accidental, or unlawful (1) misuse of User accounts for the Licensed Software, (2) changes by the Licensee (**or by any third-party artificial intelligence or automated programs enabled by Licensee)** to the Licensed Software or its database, or (3) software scripts from being added to the Licensed Software or its database by the Licensee. Licensee is also solely responsible for, and shall indemnify, defend and hold harmless Licensor regarding any Loss Event Expenses that arise from unlawful or accidental access or disclosure of Customer Data that is stored on a computer system, network, server, workstation, PC, desktop, notebook, or mobile device of the Licensee or one of its agents or contractors (other than Licensor or one of its agents or contractors). Section 6.2 ("Licensor Responsibilities") shall apply to Customer Data stored on computer systems of License or one of its agents or contractors.

5. Entire Agreement; No Other Modifications.

Except as expressly modified by this Amendment, all terms and conditions of the License Agreement shall remain in full force and effect, unamended and unaffected.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the Effective Date.

Licensor:	**Licensee:**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Attachment 1: Statement of Work

Solano County Probation

and

Journal Technologies, Inc.

Section 1 – Introduction

This Statement of Work ("SOW") effective as of the date of last signature below sets forth the framework to implement the eProbation On-Premise Environment migration to AWS GovCloud for Solano County Probation (herein referred to as "Client"), by Journal Technologies, Inc. (hereinafter referred to as "JTI").

This SOW describes the scope of the project, its phases, and assignment of responsibilities, as well as the required deliverables by the Client and JTI.

Section 2 – Project Scope and Definition

2.1 Project Scope

The project scope includes requirements, development, testing and delivery of on-premises database and file migration (eProbation environments) to AWS GovCloud for the Client.

Applications/Environments	
	1. eProbation Production 2. eProbation UAT/Test (AUX) 3. Public Portal 4. File Migration
Databases	
	1. eProbation Production 2. eProbation UAT/Test (AUX) 3. Public Portal
Interfaces (JTI Cloud Hosting does not allow incoming SQL connections/views that are currently deployed within the On-Premise environment)	
	1. ARIES – ***Out of Scope*** 2. ATIMS a. Arrest Notification b. Booking Roster (Sheriff) c. Alternatives to Custody (ATC) Report 3. CE Assessments, CE Planning, CE Programs and CE Provider (Catalis, formerly Automon) - ***Out of Scope*** **4.** DCSS - ***Out of Scope*** 5. Level II MAGUS 6. OffenderLink 7. Sentry 8. Contexte (CourtCal) – eCourt events 9. eCourt Pretrial E2E 10. eCourt E2E Justice Partner View 11. TouchPay
Active Directory/SSO - eProbation access	
	1. LDAP/AD a. Entra ID (MS AD cloud Single Sign On) for eProbation environment
VPN/Whitelisting – Options:	

	1. VPN: Site-to-site VPN with end point devices and configuration/Data in transit 2. Whitelist general user IP Range

The migration scope includes the transition of all on-premises application and database components related to the eProbation environment to the JTI-hosted AWS GovCloud platform. This encompasses:

2.1.A Applications:

- eProbation Production, UAT/Test (AUX), Public Portal and File Migration

2.1.B Databases:

- Associated databases for each application.
    - Databases contain ALL the current configuration, workflow processes, and current client data will be migrated to the AWS GOV Cloud Database and Application Server
    - Documents and files stored in the DMS will be migrated to the AWS GOV Cloud S3 storage.
    - Public Portal environment will be transferred to the AWS GOV Cloud Application Server.

2.1.C Interfaces:

- Integration with external systems currently utilizing SQL views:
    - ARIES: ***Out of Scope***
    - ATIMS
    - CE Assessments, CE Planning, CE Programs and CE Provider (Catalis, formerly Automon): ***Out of scope***
    - DCSS: ***Out of Scope***
    - Level II MAGUS
    - OffenderLink
    - Contexte (CourtCal): ***Replaced with E2E***
    - TouchPay
- Due to JTI Cloud Hosting restrictions, inbound SQL connections/views are not permitted, requiring alternative secure data exchange methods for an additional cost as identified in Section 3.1.B.
- Client has provided interface specifications and requirements attached to this SOW as individual appendixes.

2.1.C.1 Interface Narratives

- ARIES
    - Client no longer requires this interface.

- ATIMS
    - The integration between Solano County's Jail Management System (ATIMS) and the Probation Case Management System (eProbation) facilitates the exchange of **arrest, custody, and custody status data** to support probation officer notifications, pretrial services, and Alternatives to Custody (ATC) program operations. Currently, these interactions rely on direct database connections and file exchanges between on-premise systems. With the transition to cloud-hosted environments, new methods such as secure file transfer or API services will replace legacy connections to ensure reliability and vendor support.

      Exchange 1 – Arrest Notification
      When an individual is booked in ATIMS, the system attempts to identify a match in eProbation and notifies the assigned probation officer. In the future model, ATIMS will generate a structured booking record (XML/CSV) and securely deliver it to eProbation. eProbation will process the record, send notification emails to the responsible officer(s), and optionally create in-application alerts or queue cases for manual review. This shift centralizes notification handling in eProbation, improves reliability, and removes dependencies on direct email integration and synchronous system availability.

      Exchange 2 – Booking Roster
      Today, eProbation directly queries ATIMS for recently booked individuals to populate its Booking Roster. In the new design, the same booking feed used for arrest notifications will also populate the Booking Roster, therefore eliminate duplicate data paths and reduce maintenance overhead. This approach consolidates processes to a **single inbound booking feed** from ATIMS.

      Exchange 3 – Alternatives to Custody (ATC) Report
      ATC officers currently generate a Crystal Report by merging ATIMS custody data with eProbation case information through direct database queries. In the future model, integration options include either (1) implementing an API call from ATIMS to eProbation at runtime for real-time case data retrieval and report merging, or (2) making ATC-related data available through an eProbation portal for officers to access directly. Both approaches eliminate the dependency on direct database connectivity and support modern, cloud-hosted operations.

      Collectively, these redesigned interfaces will provide a **modern, secure, and supportable integration** between ATIMS and eProbation, ensuring uninterrupted delivery of arrest notifications, pretrial case intake, and custody program reporting in a cloud environment.

- CE Assessments, CE Planning, CE Programs and CE Provider (Catalis, formerly Automon)
    - With the replacement of Catalis (formerly Automon) functionality defined as an existing deliverable, **Client is opting to forgo development** of this interface when migrating to hosted services.

- DCSS
    - Client no longer requires this interface.

- Level II Magus
    - The CLETS interface provides an outbound integration between Solano County Probation's eProbation case management system and the County's Message Switch System (LTI MAGUS), which connects to DOJ CLETS and local law enforcement CAD/dispatch platforms. This interface enables law enforcement agencies to receive timely probation "CLETS returns" directly through their existing systems, eliminating the need to separately query eProbation.

      The return includes essential demographic information, officer safety alerts, case status, probation conditions, and supervising officer assignments for adults and juveniles on probation or with pending cases. Information is concise and standardized, ensuring compatibility with CLETS while prioritizing officer safety and operational efficiency.

      The interface will be implemented using a REST API–based approach, replacing legacy SQL views with modern eProbation views. It is triggered automatically when designated CLETS queries (e.g., person checks) are detected by MAGUS, parsed for required identifiers, and routed to eProbation. Responses are then returned through MAGUS to the originating law enforcement system. If, and where possible, JTI will leverage the eCourt configuration of their interface with Level II Magus.

- OffenderLink
    - The OffenderLink interface is a **bi-directional, file-based integration** between eProbation and the OffenderLink supervision platform, supporting both client enrollment and supervision activities. The interface enables probation staff to enroll, update, suspend, or remove clients in the OffenderLink program directly from eProbation, while also importing program updates and appointment notifications from OffenderLink back into eProbation.

      On the **outbound side**, eProbation generates nightly data extracts (e.g., offender, sentence, offense, warrant, employment, and appointment files) that are securely transmitted via SFTP to OffenderLink. These files ensure that clients enrolled in OffenderLink — including those under specialized caseloads such as Pretrial and Domestic Violence — are properly flagged and synchronized. Data rules handle multiple phone numbers, addresses, and caseload assignments, with specific exclusions to maintain program alignment.

      On the **inbound side**, OffenderLink provides nightly files containing client updates and appointment information, which are processed into eProbation. This supports **automated client notifications** (e.g., Pretrial appointment reminders) and ensures probation officers can view accurate supervision data within eProbation. Business rules in eProbation govern file exchange, validation, and data mapping to guarantee completeness and consistency.

JTI will **leverage configuration patterns and lessons learned from prior implementations** with FieldWare (OffenderLink's vendor) and other JTI customers to streamline development, reduce risk, and ensure that the OffenderLink integration is deployed efficiently and in alignment with industry best practices.

This interface replaces legacy file exchanges with modernized processes while retaining the same program workflows. It ensures accurate enrollment management, supports court-ordered supervision, and enhances client engagement through automated notifications — all while leveraging secure, auditable file transfer mechanisms suitable for a cloud-hosted environment.

- Cordant/Sentry
    - The Cordant Sentry integration is an **inbound SOAP API interface** that delivers drug test results from Cordant's certified laboratory system directly into Solano County's eProbation case management system. This interface supports probation operations by ensuring timely, secure, and accurate transmission of laboratory data for individuals under supervision.

      Cordant transmits drug test results using a SOAP-based service (getResults method), with end-to-end encryption via TLS 1.2. Results include demographic and case identifiers (e.g., case number, name, DOB), group assignments, test metadata (date ordered, date tested, lab number, type, and status), and detailed drug results. These results are imported into eProbation every 30 minutes through an automated business rule, populating a **read-only Drug Test form** within the application for officers to review.

      In the new cloud-hosted model, no functional changes are required to the interface itself — only updates to endpoints and connectivity configurations. This maintains existing workflows while ensuring compatibility with cloud infrastructure and CJIS-compliant security requirements.

      The Cordant Sentry interface ensures that probation officers have seamless access to certified lab test results within eProbation, enhancing reliability, eliminating manual data entry, and supporting supervision, compliance monitoring, and court reporting needs.

- CourtCal (Contexte)
    - The Court Calendar interface is an **inbound integration** that delivers court scheduling and outcome information from Solano County's court systems into eProbation. This integration ensures that probation staff have timely and accurate visibility into hearings, case events, and related outcomes without relying on paper-based calendars or manual data entry.

      Currently, the interface is supported by a combination of a file drop via ETL (from the Court system) and SQL Server jobs/tables (within Solano County) that capture future hearings and outcomes on a nightly basis. These records are then made available to eSuite applications within the county via read-only access.

The requested enhancement will modernize the interface by converting it into a **REST API–based integration**. Future court events will be delivered as they are scheduled, and past hearings will be updated with results or outcomes, using the **court case number as the primary identifier** for synchronization. This shift from batch-based database queries to event-driven API updates from eCourt ensures more timely and reliable availability of calendar data in eProbation.

JTI will **leverage prior experience implementing eSeries 2 eSeries API court calendar integrations** for other customers, applying proven patterns to Solano's requirements to streamline development and reduce risk. This will provide a secure, efficient, and supportable solution aligned with modern best practices and a cloud-hosted model.

- TouchPay
    - The TouchPay interface is an **outbound, file-based integration** between eProbation and the TouchPay payment platform. This interface enables clients to make restitution, fines, and fee payments through multiple channels — including probation department kiosks and the TouchPay website — while allowing near real-time account balance lookups based on client account numbers.

      On a scheduled basis (every 30 minutes), eProbation generates a **delimited text file** containing client account data (name, DOB, SSN, case type, account number, and balance due). These files are transmitted via **secure SFTP** to TouchPay, where they are used to update client accounts for payment processing. Each file is uniquely time-stamped, ensuring accurate reconciliation of records.

      At the end of each business day, probation accounting staff reconcile payments recorded through TouchPay (website, kiosk, or in-person) against client balances in eProbation.

- eCourt Pretrial E2E
    - The **Solano Pretrial – Court Data Exchanges project** enhances integration between eProbation and eCourt through a series of interfaces designed to streamline pretrial processes. The scope covers automated exchanges of case data, hearing outcomes, document submissions, status updates, and bench warrant handling, reducing manual workload while ensuring timely and accurate information sharing between the systems.

      Key functionality includes the ability to carry arraignment case numbers from eCourt to eProbation for use in Pretrial Services Reports and Contracts, as well as exchanging post-arraignment status outcomes and supporting documents. eProbation gains the ability to submit pretrial documents directly to eCourt, with version control, acceptance/rejection handling, and confirmation receipts. Conversely, eCourt provides probation with updates on Pretrial Services status changes (e.g., continued or terminated) and the supporting court documents.

- eCourt E2E Justice Partner View
    - Partner integration allows for running searches, folder views, headers, or document downloads from another agency or client's eSeries application. The partner application

integration is done using APIs and requires that the partner application is a reachable network to the calling eSeries application.

- The system provides three endpoints for doing partner integration:
  - Search API
  - Folder View / Header API
  - Document download

2.1.D Active Directory/SSO:

- Integration with LDAP/Active Directory utilizing Microsoft Entra ID (previously known as Azure AD) for Single Sign-On (SSO) for additional cost as identified in Section 3.1.B.

2.1.E VPN and Whitelisting options:

- Implementation of secure site-to-site VPN access, configuration of endpoint security, or IP range whitelisting for authorized user access.

2.2 Out of Scope

2.2.A Disclaimer on Scope Alignment

The exclusions listed below are consistent with the terms of the *Journal Technologies Software License, Maintenance, and Support Agreement* executed with Solano County.

Under that agreement, Journal Technologies provides maintenance and support for the licensed application software only, and not for customer-managed infrastructure, database systems, or custom code development outside of standard configuration capabilities within the Journal Technologies framework.

Any services or enhancements falling outside of this scope may be provided under a separate **Professional Services Agreement**, subject to mutual agreement of the parties.

2.2.B Out of Scope

The project will be limited to the scope of work described in **Section 2.1**. The following items are **expressly excluded** from the scope of this engagement and will not be provided under this Statement of Work:

1. **Infrastructure and Database Support**
   a. Any installation, maintenance, troubleshooting, or support related to **Solano County's on-premises infrastructure**, including but not limited to hardware, network configuration, database administration, operating systems, backup, and disaster recovery procedures.
2. **Functional Enhancements Beyond Defined Scope**
   a. Any requests that introduce **new business functionality**, workflows, or processes **not identified in Section 2.1**, or that modify existing functionality beyond the agreed scope.

3. **User Interface and Aesthetic Changes**
    a. Any requests pertaining to the **visual design**, layout, or styling ("look and feel") of the application, except where explicitly specified in this SOW.
4. **Unrelated or Unapproved Customizations**
    a. Development or modification of **existing production configurations** or functions that are **unrelated to the defined project deliverables,** or the interfaces identified in Section 2.1.
5. **Core or Source Code Development**
    a. Any development or modification to the **core application codebase** or any component **not supported through standard configuration within the Journal Technologies framework**.
    b. Enhancements or changes requiring **alteration of base software modules, compiled code, or system architecture** are expressly excluded and would require a separate **Professional Services Agreement**.

2.3 Project Phases

The project will follow JTI's standard methodology for migrating the Client's on-premises environment to JTI-hosted AWS GovCloud. Regarding updates to current on-premises data exchanges needed to support AWS GovCloud security compliance, JTI will follow the process defined below for implementing initiatives.

- A new JIRA ticket will be created for each initiative, and time will be tracked against it, including time to document/assess the requirements.
- JTI and the client will evaluate current interface methods (e.g., SQL views, HTML/JSON APIs, SFTP CSV exchanges) and map relevant business processes and data flow dependencies
- Each initiative will be documented via an interface requirement or work request document. (see template in Appendix A, B).
- Upon receipt of the approved initiative, work request, or email, JTI will move the work into the configuration backlog for planning.
- JTI will complete the necessary work to deliver the initiative including unit testing of the solution.
- Client will begin system testing against the requirements defined in the work request or email.
- Client will report issues to JTI where the delivered initiative does not match the requirements within 5 workdays.
- JTI will make the appropriate configuration changes to address the reported issues.
- In the event the solution requires development resulting in the need to upgrade to a later version of eSeries or the Portal, the software will be deployed to the TEST environment, and the Client system testing will include regression testing.
- There will be a maximum of two iterations spanning 15 days each for testing, unless a reported issue is outstanding which prevents the initiative from being moved to production.
- JTI (and/or Client) will schedule / move the initiative to production.
- Client will validate the initiative in production.

Lead Time: JTI requires a minimum of 45 days to plan, prepare, and provision environments in AWS GovCloud.

Section 3 – Project Cost and Billing

3.1 Cost

3.1.A JTI will bill the Client a one-time fee of $20,000.00 for eProbation application migration and $10,000 for Public Portal migration services described in 2.1.A and 2.1.B.

3.1.B JTI will provide up to 900 hours of additional services at the current rate of $200 per hour. For reconfiguring LDAP to use Microsoft Entra ID for Single Sign-On (SSO) and reconfiguring listed interfaces to use supported exchange methods as described in 2.1.C. Deliverables will be invoiced upon signing of the acceptance document. Such additional required hours are available through December 31, 2026 and will be billed on a time and materials basis at $200 per hour based on the billing terms in section 3.2, including the analysis of current interfaces and the identification of existing data exchange methods (e.g., SQL views, HTML or JSON API exchanges, and CSV file transfers via SFTP).

Interface	**Amount**
ATIMS	$60,000.00
Level II MAGUS	$60,000.00
OffenderLink (FieldWare)	$30,000.00
Contexte (CourtCal): Replaced with E2E	$0
TouchPay	$20,000.00
LDAP/Entra ID	$10,000.00
Interface SubTotal	$180,000.00
eProbation Application Migration	$20,000.00
Public Portal Migration	$10,000.00
TOTAL SOW	**$210,000.00**

3.1.C Hosting fees will be assessed at a monthly pro-rated 1/12th the annual amount once the AWS GovCloud environment is created and accessible.

3.2 Billing Terms

The Client will be invoiced based on the following payment milestones upon acceptance of each deliverable found in the chart in section 3.1.B.

If additional scope or hours are deemed necessary by JTI and the Client, those hours will be invoiced monthly. The invoice will be itemized by date, resource, hours, and service(s) provided. In the event the hours are not allocated by December 31, 2026), a new statement of work will be required.

Section 4 – Assumptions

Migration of the on-premises applications and databases for the Client is per the following assumptions:

- The client will provide security protocols/access to non-Production servers.
- The client will test in a non-Production environment.
- The client will provide security protocols/access to the Production server.
- The client will test in the Production environment.

Implementation of the time and materials hours for the Client is per the following assumptions:

- JTI reserves the right to reject an initiative work request if it is determined to be out of alignment with the eSeries product roadmap or framework.
- The client will complete system testing and provide JTI with timely feedback.
- The client will complete regression testing if applicable.
- The client will complete a final validation of the delivered solution in the production environment.
- To the extent possible, the core eSeries solution will be utilized to be as efficient as possible.

Section 5 - Project Management

JTI will keep the Client updated on the status of the migration on a regular basis. The Client will have access to JIRA to view updates on items that have been submitted.

IN WITNESS WHEREOF, the parties have caused this instrument to be duly executed as of the date last written below.

Dean Farrah, Chief	Date
Solano County Probation 475 Union Avenue Fairfield, CA,94533	
Jon Peek, Senior Director of Professional Services Journal Technologies, Inc.	Date

EXHIBIT D
HOSTED SERVICES

Licensor Hosting. In consideration for Licensee's payment to Licensor of the Annual Hosting and Storage Fees (in addition to the Annual License, Maintenance and Support Fees) set forth on **Exhibit A**, Licensor will provide Licensed Software hosted services (the "**Hosted Services**"), which Licensee may access via a secure Internet connection.

Definitions. Capitalized terms used and not otherwise defined in this **Exhibit D** shall have the respective meaning given to them in the Agreement.

Licensor Responsibilities. Licensor's responsibilities with respect to the Hosted Services are as follows:

a. Provide Software as a Service (SaaS) for the hosting of Licensee data, in keeping with the definition of SaaS set forth in NIST Special Publication 800-145.
b. Provide Maintenance of the Hosted Services.
c. Provide services as described in this **Exhibit D**.
d. Licensor shall not be responsible, for any accidental or unlawful access or disclosure of confidential Customer Data that results from Licensee's failure to comply with subparagraph b. below under the heading "Licensee Responsibilities."

Licensee Responsibilities. Licensee's responsibilities with respect to the Hosted Service are as follows:

a. Pay the Annual Hosting and Storage Fees listed in **Exhibit A**.
b. Provide a secure internet connection between Users and the hosted environment that meets necessary bandwidth requirements.
c. Licensee is solely responsible for, and shall indemnify, defend, and hold harmless Licensor regarding, any unlawful or accidental access to or unauthorized or improper disclosure of Customer Data that results from (i) the conduct of an authorized User of Licensee, (ii) an unauthorized person obtaining an authorized User's account credentials from such a User or Licensee, (iii) changes that Licensee makes to the configuration of the Licensed Software or the hosted database, or (iv) software scripts added to the Licensed Software or the hosted database by Licensee. Without limiting the foregoing, Licensee shall: (A) notify Licensor immediately of any unauthorized use of any password or account or any other known or suspected breach of security; (B) report to Licensor immediately and use reasonable efforts to stop immediately any copying or distribution of content that is known or suspected by Licensee or Users; and (C) not impersonate another User or provide false identity information to gain access to or use the Hosted Service.

d. Accept that Licensee and any and all third parties associated to the Licensee (i) will never have direct, privileged access to Licensor's hosted infrastructure (servers, database, file storage, AWS monitoring, AWS dashboards) and accordingly (ii) are restricted from installing or requiring installation of third-party software.

e. Accept that each hosted instance allows for one (1) terabyte of database storage. Licensee will be notified when database storage usage thresholds exceed 80% of the then available storage and the database storage will be expanded in accordance with **Exhibit A** upon Licensee approval. If Licensee does not approve increased database storage space beyond one terabyte (1TB), such additional space will not be provisioned; Licensee will reduce its use as needed to remain within the allotted 1TB. In Licensor's experience, 1TB is virtually always ample space for a customer's database. Additional database storage may be pre-purchased at any time.

f. Accept that each hosted instance allows for one (1) production environment and one (1) auxiliary environment. Additional environments requested by Licensee shall be subject to additional costs.

g. Have and maintain the following workstation configuration requirements:

Component	**Minimum Specification**
Processor	1 @ 2.0 Ghz or faster
Hardware	Mouse/trackpad, keyboard
Memory	4 GB minimum (8+ GB preferred)
Monitor Size	Minimum resolution: 1600x1200
Video Card	Standard
Disc space	100 GB minimum
Network	Secure internet connection
Operating system	Supported OS from Microsoft or Apple
Other required software and versions	Supported browser versions of Licensee's choice from the following list: Microsoft IE, Microsoft Edge, Firefox, Google Chrome, Apple Safari. Java Runtime Environment 8 only for automated printing and scanning.
Third-party applications and versions, what they are used for	MS Word, Adobe (This is for viewing and generating documents in Word and PDF format)

System Period of Maintenance.

a. *Weekly Maintenance Window* (Wednesday, 9:00PM to Thursday, 4:00AM PT). The Hosted Service shall be subject to a maintenance window each Wednesday evening or as agreed upon by Licensee. Hosted Service maintenance window may include loss of

network access, the servers, and the operating system during such window. The Hosted Service will not always be disrupted during each weekly maintenance window.

b. *Extended Maintenance Outage***.** If Licensor requires additional time for maintenance or installation, Licensor shall provide written notification to Licensee at least 24 hours prior to implementing an extended maintenance outage. Licensor's notice shall explain the nature and expected duration for the extended maintenance outage.

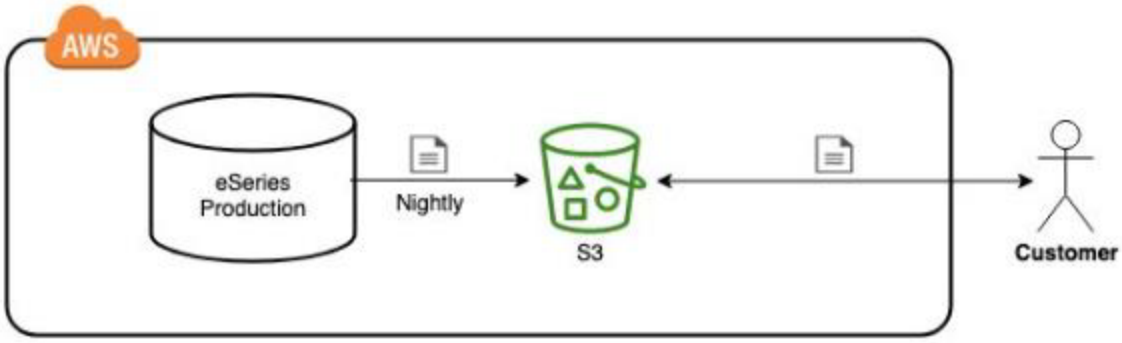
c. *Critical Security Maintenance*. The Hosted Service shall be subject to immediate security maintenance with less than 24-hour notice given to the Licensee in the event a critical software vulnerability needs to be patched.

Licensor leverages world class cloud infrastructure provider Amazon Web Service (AWS) to host Licensee data and software. AWS provides state-of-the-art compute power, storage and security. Licensor's cloud hosting service results in a higher level of security, availability, fault tolerance and disaster preparedness than is generally available with on-premise solutions.

DATABASE STORAGE

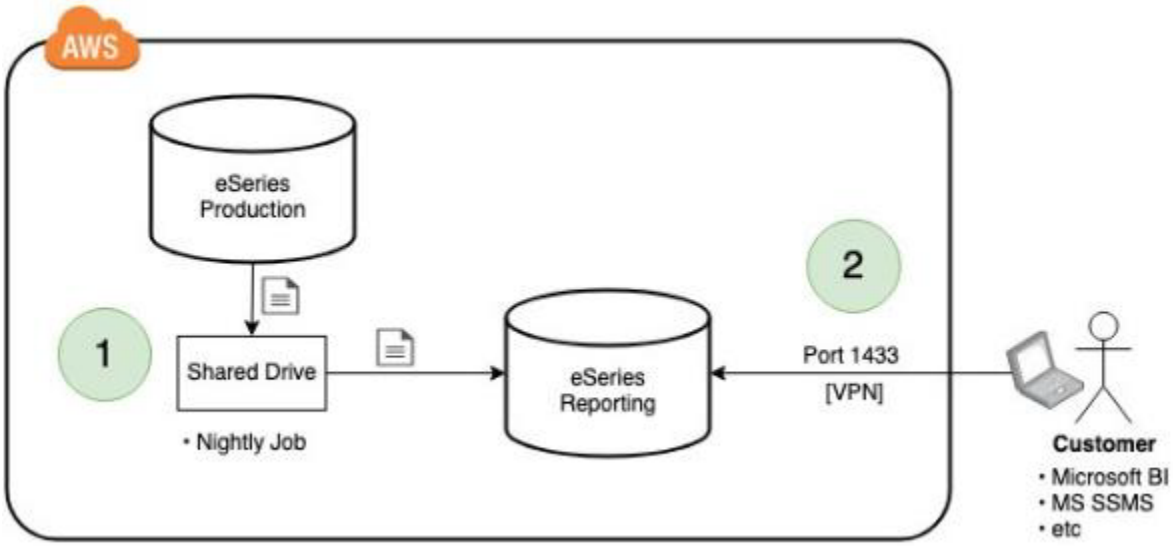
One terabyte (TB) of database storage is included with the hosting service. Additional database storage is always available and is automatically provisioned when required. At the end of the current billing period, Licensor compares the actual storage Licensee is using to the contracted amount and, if necessary and only following notice to and approval from Licensee (i) adjusts the storage cost for the next period and (ii) may retroactively bill the Licensor for the actual usage, per the database storage rate table in **Exhibit A**. Licensee acknowledges that if it does not approve increased database storage space beyond one terabyte (1TB) that such additional space will not be provisioned and Licensee will reduce its use as needed to remain within the allotted 1TB. In Licensor's experience, 1TB is virtually always ample space for a customer's database.

Nightly database backups are available to the Licensee upon request at no additional cost. Licensor will export data using standard data formats to a location the customer may download from AWS S3. Each day's copy overwrites the previous nights. These backups can be used at the Licensee's discretion such as running Business Intelligence tools such as Microsoft BI or Tableau. Licensee can also provide interfaces to other justice partner agencies, provided that Licensee must honor all non-disclosure terms of this Agreement as well as responsibilities associated with all applicable federal, state, and local laws in connection with data protection.



At Licensee's election and for an additional cost (currently $1,245 per month but subject to change upon 60 days' notice), Licensee may pay for a second, dedicated database which is restored nightly with production data every 24 hours. The database is hosted by Licensor in our AWS GovCloud. With this option:

- Customers access the database via tools hosted on their own systems.
- Customers may only provide access to their own agency users (no 3rd party agencies).
- Journal Technologies does not provide support for the tools used by the Customer.
- Data storage counts against the Customer's contractual allocation.
- Connects to BI Database Server via standard port 1433 through VPN.
- A maximum of 5 end-users per customer will be provided read-only access.



DOCUMENT STORAGE

Licensor provides on-demand document storage to meet the Licensee's document management requirements. Licensor leverages world-class document storage solution AWS to store documents. Licensees are billed for the storage they use ("pay as you go") with no storage caps. The system is designed to optimize Licensee storage costs by automatically moving documents and objects to cost-effective access tiers without little performance impact or operational overhead.

Document storage incorporates three access tiers: *Frequent Access, Infrequent Access,* and *Archive Access*. Documents that have not been accessed for a minimum 30 days are automatically moved to the *Infrequent Access* tier. Documents that have not been accessed for a minimum 90 days are automatically moved to the *Archive Access* tier. If the Document is requested, it will be moved back to the *Frequent Access* tier and the lifecycle begins again.

Licensees can store any number of documents and are automatically billed according to the rate table in **Exhibit A**. Each document object can be up to 5 TB in size and is replicated automatically across multiple data centers for redundancy. All objects are versioned protecting data from the consequences of unintended overwrites and deletions.

Copies of the systems complete document file store are available upon request for a transfer fee of $40/Day + $0.20 USD/GB with a minimum of 10 calendar days to complete extraction. Shipping and handling will be added. For this extraction, all documents and other digital files stored in the case management system will be copied to an encrypted hard drive and delivered via a certified carrier. Transfer fee is subject to price change throughout the course of this agreement, not to exceed the Bureau of Labor Statistics CPI increase for Client's region (West Region) for the period intervening any increase upon 60 days prior notice.

SECURITY

Secure Hosted Environment - AWS offers an environment specifically for government applications called AWS GovCloud (US). GovCloud is an isolated AWS region designed to host sensitive data and regulated workloads in the cloud, helping customers support their U.S. government compliance requirements, including the International Traffic in Arms Regulations (ITAR) and Federal Risk and Authorization Management Program (FedRAMP). GovCloud is operated solely by employees who are vetted U.S. Citizens on U.S. soil. Root account holders of AWS accounts must confirm they are U.S. Persons before being granted access credentials to the region. All GovCloud data centers are in the continental United States. GovCloud, in conjunction with other security and procedural practices, helps to create a JTIS and FIPS 140-2 compliant environment. More information about GovCloud is available at https://aws.amazon.com/govcloud-us/

Data Security – Journal Technologies builds our hosted solution to meet data security standards and best practices set forth by the US Department of Justice Criminal Justice Information

Services (CJIS) Security Policy. We also reference *Security Control Mapping of CJIS Security Policy Version 5.9 Requirements to NIST Special Publication 800-53 Revision 5* a mapping represents a "best fit" correlation between the CJIS Security Policy controls and NIST federal controls.

Data at Rest - The database in our hosted solution is attached to an encrypted volume with a data key using the industry-standard AES-256 algorithm.

Data in Transit - Journal Tech customers are hosted in AWS GovCloud (US). The connection to Licensee's location is established using a site-to-site virtual private network (VPN) or over HTTP over TLS (HTTPS). When CJI is transmitted outside the boundary of a physically secure AWS data center, the transmission is encrypted utilizing FIPS 140-2 compliant ciphers with a symmetric cipher key strength of at least 128-bit strength.

Security Testing – Licensor runs nightly vulnerability scans on our hosted infrastructure. This includes scans for vulnerabilities such as OWASP exploits, weak authentication, operating system and application versions, etc. It also checks for suspicious behaviors (or indicators of compromise) which are programs or people doing activity they don't normally do such as escalating privileges, logging into a server a named user never uses, accounts running scripts they previously did not, etc.

Licensor undergoes monthly, internal penetration and vulnerability tests across our product lines using NIST 800-30 to assess the overall risk of any vulnerabilities found. Guidance for vulnerability tests come from the OWASP Application Security Verification Standard (ASVS) 4.0.

Security Breach - A security breach is an incident that results in unauthorized access to data, applications, networks or devices. In the event of a potential security breach, Journal Technologies will follow its Security Incident Response Plan. If a verified security breach occurs Journal Technologies will promptly notify client IT representatives or CSO.

SOC 2 Type 2
Licensor has completed a System & Organization Control (SOC) 2 Type 2 audit, an independent third-party examination of Licensor's information security controls. Licensor can make available to Licensee Licensor's most recent SOC report (or, if desired by Licensee, additional historic reports) upon Licensee's request therefor, subject to the confidentiality provisions of this Agreement and any other procedures Licensor may deem necessary to protect the security of such reports.

DATA OWNERSHIP
All the hosted Customer Data remains Licensee's property during and after the lifetime of the hosting contract. Licensor interaction with Customer Data strictly limited to supporting Licensee's operation.

DATABASE BACKUPS AND DISASTER RECOVERY

We backup your production database every two hours to redundant storage available in multiple availability zones. At the end of the day, the final backup is archived, and the other hourly backups are overwritten the next day. We maintain fourteen days of archival data backup.

This gives us a Restore Point Objective (RPO) of two hours or less.

We snapshot your running Compute Instances (CI) once every 24 hours and rotate the CI backups every 14 days.

All backups and snapshots are encrypted at rest.

In a disaster scenario, should your compute instances in the primary availability zone cease to respond for two hours we begin to restore from backups and snapshots to a different availability zone.

Our DR Restore Point Objective (RPO) is two hours or less and our Recovery Time Objective (RTO) is twenty-four hours or less

CLOUD MAINTENANCE

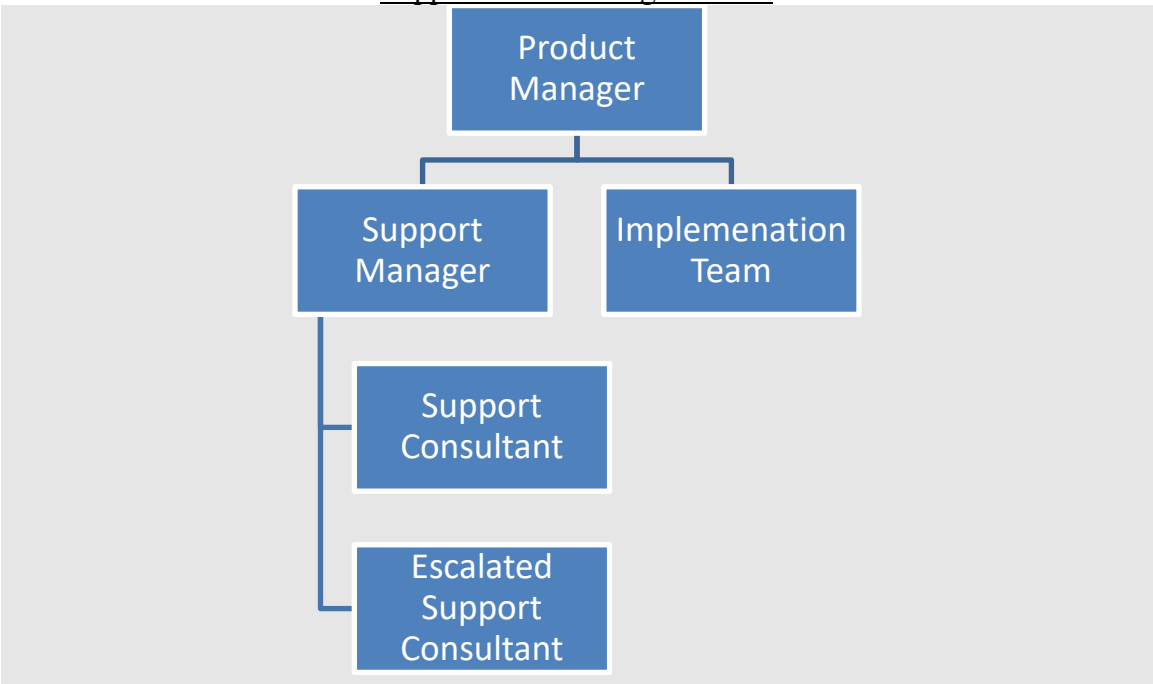
Journal Tech (i) installs operating system (OS) updates as needed during maintenance windows and (ii) install critical OS updates within 24-48 hours of a CVSS score of 7 or above.

Amendment Attachment 3

Exhibit E - Service Level Agreement

In-house support staff are located in Logan, Utah and work closely with our implementation teams, and report to the same product manager.

Support Services Organization



Support Case Life Cycle

During the implementation, your JTI Support Manager will work closely with your implementation team and get to know your eSeries Administrators to help gain an understanding of processes, business rules, workflows and interfaces.

To ensure a smooth transition from Implementation to Support, there is a transitionary period of about 90 days or more after your go-live where your Implementation Team will continue to provide support. Upon acceptance of your implementation project, where you are running stable, you will fully transition to Support. After your transition to Support, Implementation personnel will continue to be available via an escalation path to help provide solutions.

Your eSeries System Administrators and Help Desk personnel are trained during the implementation to maintain your JTI products and become the front line of support for your end users. A built-in help function provides context sensitive help as well. Your authorized Administrators can access our support staff via toll-free phone, email and online web portal. Administrators can create new support cases, view and update active cases, upload files, and view previously solved cases.

We are passionate about your phone calls never having to go to voicemail. Our streamlined call answering tree continues to roll over and expands to include additional staff.

All support issues are logged into a Support CMS, which stores customer information including contracts, go-live dates, designated eSeries administrators, etc. Every support case is assigned a case ID, time and date stamped, and it has a history of notes, correspondence, parties and solution information. Case information is accessible online through our support portal.

We immediately acknowledge receipt of your request, including a case ID for call tracking purposes. If the request is categorized as "Critical" we will provide a solution through a service release in accordance with the Incident Response and Resolution table below.

Troubleshooting to obtain reproducible steps of a critical application error begins immediately. Troubleshooting for all other application errors are typically based upon priority categories (see "Incident" definition section below). We work closely with your eSeries Administrator while resolving each support request. When necessary, cases are escalated to our seasoned Escalated Team and then to the Development team as indicated in the subsequent Support Case Flow diagram. Nearly all issues can be resolved remotely, rarely requiring a need for onsite support. Onsite support is available when necessary.

We utilize numerous remote diagnostic tools to assist in solving support cases. Screen sharing tools are typically used for remote troubleshooting. These tools provide the advantage of remotely gathering system information, reconnecting after reboot, secure file transfers, and requesting escalated permissions when needed. Our applications log errors used for troubleshooting and debugging.

Data logging tables capture changes made to the database and may also be used for troubleshooting. Java Virtual Console monitors memory and thread usage, SQL Profiler traces, Tomcat access logging, Microsoft Windows Perfmon and others are common diagnostic tools used for troubleshooting.

Throughout this process your Support Manager and Consultant updates you on the progress. Also, automated notifications are sent with each status update.

Upon solution verification from your approved Administrator, the support case is time and date stamped as closed, and an automated notification is sent to your eSeries Administrators with the solution. (A link is included in all notifications to allow feedback to the Support Manager.)

Enhancements/Updates

Enhancements/new feature requests are submitted by your system administrator through the Customer Support Department. They are evaluated by JTI's Product Owners and, if selected, the feature is made available in a future release.

You are eligible to receive software updates as part of your current maintenance. You will be notified of update availability through standard communication channels, website, support portal, or email. You will retain complete control of the timing and process of any updates. Updates are typically completed within one hour.

For cloud-hosted solutions, applying updates will be performed by JTI, and timing will be coordinated with and approved by your office. We will test and verify business processes in the new version to ensure they are fully operational in a non-production environment, perform a system/database backup, then schedule the production upgrade.

Because eSeries is configurable, changes to accommodate situations such as new legal requirements may be accomplished by your system administrator and/or IT Staff. The changes are generally completed in a non-production system, tested, then transferred to the production with little to no impact on case processing. New feature/configuration change requests submitted to JTI will be pursuant to a Statement of Work.

Services that go beyond routine Support may be provided under the terms of a professional services agreement upon agreement of the parties.

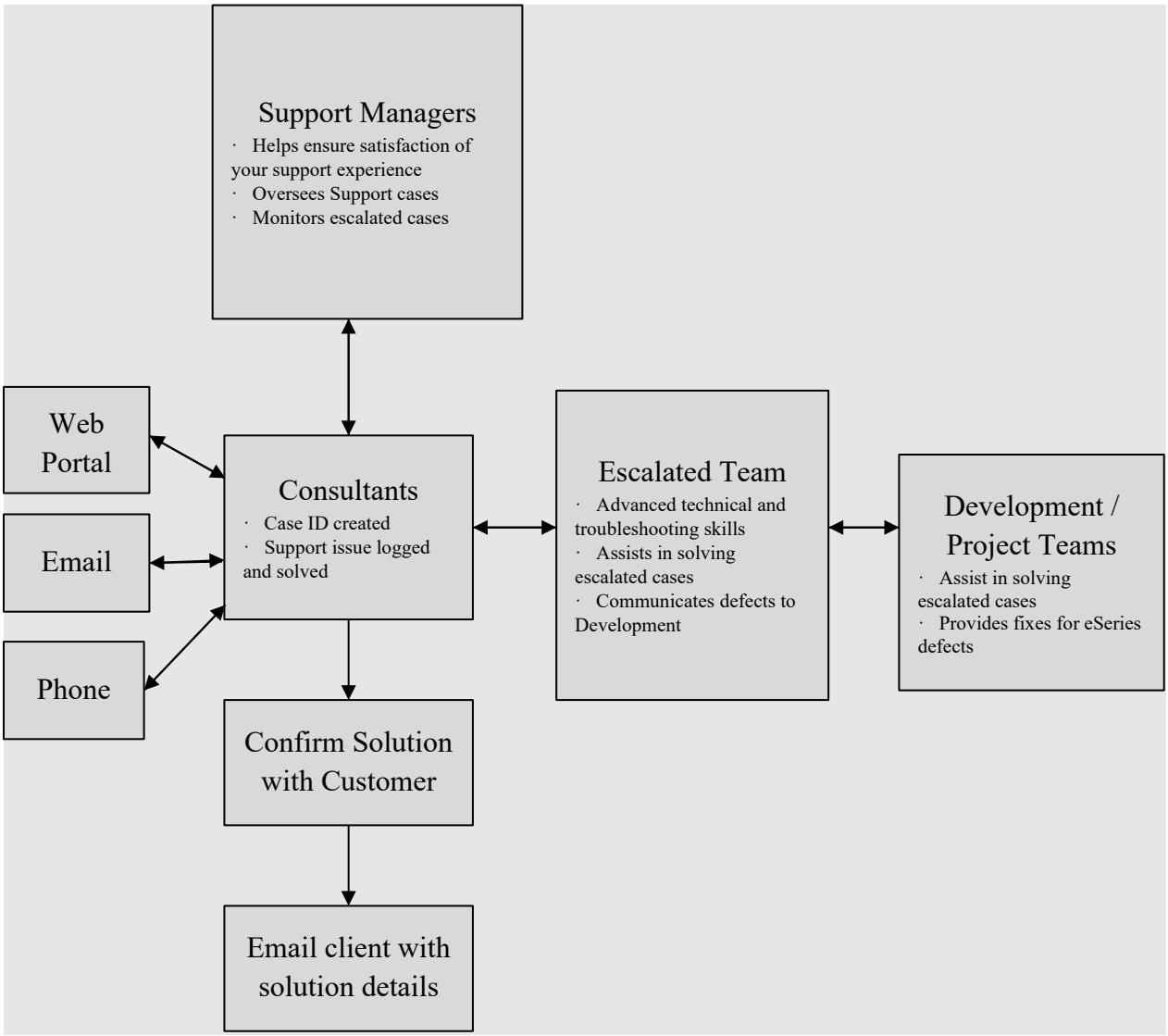
Rolling back an update requires restoring from the software and database backup that was made immediately prior to the upgrade.

Customer System Administrators

At least one authorized eSeries System Administrator is required, typically two to four; with a recommended maximum of five. These administrators are those you authorize to submit tickets to JTI Support. Additional internal support staff may be helpful to assist these system administrators.

System Administrators should have authority to make eSeries administrative decisions. Their skills should include a good understanding of daily processes and workflows for end-users, possess troubleshooting skills, knowledge of IT (networks, applications like Word and Outlook, browsers, etc.), and excellent communication skills (both written and verbal). During implementation, your authorized administrators should be trained on eSeries administration and software functionality.

Support Case Flow



Contact Information

Support is available from 5:00 a.m. to 6:00 p.m. Mountain time, Monday through Friday, except for U.S. federal holidays. If a critical situation occurs outside of normal support hours, Support can be reached 24/7 via an emergency extension.

Products	Phone	eMail
eSeries	877-364-0120	eSeries-support@journaltech.com

eProsecutor, eDefender, eAttorney	877-364-0121	eProsecutor-support@journaltech.com eDefender-support@journaltech.com eAttorney-support@journaltech.com
eProbation, eSupervision, eDiversion, ePreTrial	877-364-0122	eProbation-support@journaltech.com eSupervision-support@journaltech.com eDiversion-support@journaltech.com ePreTrial-support@journaltech.com
eDelivery, eFiling, ePayIt	877-364-0123	eSeries-custom-support@journaltech.com eFiling-support@journaltech.com eDelivery-support@journaltech.com ePayit-support@journaltech.com hosting-support@journaltech.com support@journaltech.com

Customer Support/Training Program

The Continuing Education Program includes courses taught by implementation and development personnel, training guides, practical exercises, training videos, visits at customer sites and regular CJIS security awareness training.

Incident

An Incident is a disruption in the normal information flow or service with the software application. Each Incident will be classified in accordance with the below categories:

- 1-Critical: Product Failure/Loss of Service: A problem with all or part of a component of the Licensed Software causing disruption to business activity preventing the use of the System, and for which no workaround exists.
- 2-High: Non-critical System failures: A fault that causes the System to not operate in accordance with Specifications, but the System remains usable with a moderate level of difficulty. Response time degradation on non-critical system components is included in this category.
- 3-Medium: Non-critical System failures: A fault causing the service to not operate in accordance with specifications but usable with a minimum level of difficulty. Will also include questions and requests for information.
- 4-Low: A minor fault causing the system not to operate in accordance with specifications, with no disruption to business activity. This category includes "Incidents" relating to environments other than production.

Incident Response and Resolution. JTI shall respond to requests for technical support received via one of the standard methods of contact. JTI shall provide a response and resolution based on the category of Incident within the time frames set forth below:

Work Type	Category	Response Goal (via Telephone)	Response Goal (email, internet)	Resolution Goal
Incident	1-Critical	Immediate	4 business hours	ASAP, but no more than 48 hours upon verification of steps to reproduce issue
Incident	2-High	Immediate	4 business hours	ASAP, but no more than 30 days upon verification of steps to reproduce issue
Incident	3-Medium	Immediate	4 business hours	ASAP, but no more than 90 days upon verification of steps to reproduce issue
Incident	4-Low	Immediate	4 business hours	ASAP, but no more than 180 days upon verification of steps to reproduce issue

A response within goal is an acknowledgement that JTI has received the Incident Report. It does not mean that the Incident has been satisfied.

Resolution Time does not include any time period(s) during which JTI is waiting on information, clarification or task completion by the customer.

Where resolution of an incident may depend upon changes being made by JTI's Product Development team to JTI's core software code, resolution of such incident may exceed the goals set forth above as reasonably made necessary by the inherent complexity of such changes

Support Services Staff

Support Manager

Our Support Manager oversees all support operations. He ensures the right staff are assigned to solve your case and monitors the progress of each case from his electronic case board. He also manages the training program for new employees and continuing education for current staff.

Support Consultants

Consultants answer and respond to phone calls, emails and Web Portal requests. They are responsible for case creation and tracking of all incidents and solving most incoming issues on the spot. They will help walk you through steps, troubleshoot problems, and provide all the information you need. When the problem is more complex, the issue will be escalated. However, the primary responsibility for the case remains with the Consultant.

Escalated Support

Escalated Support Technicians are seasoned members of the support team with advanced technical and troubleshooting skills. They assist in solving escalated cases and identify when an issue is categorized as a defect or a configuration issue. They work with Development to fix any defect. In addition, they take an active role in training and coaching the support team.