Exhibit 1 – STATEMENT OF WORK

REQUEST FOR PROPOSAL

1. **PURPOSE**

This Statement of Work (SOW) reflects the services to be provided by **< Contractor Name>**, hereinafter referred to as the “Contractor,” for the State. This SOW is governed by and incorporates by reference the terms and conditions attached herein.

This SOW describes the design and development of an Intake module that will provide county Child Welfare Agencies an easy to navigate and efficient way to record and access information regarding child abuse, neglect, and exploitation allegations and investigative findings. The Intake module will provide a modern user-friendly application that supports our strategy to provide quick, comprehensive information to make timely informed decisions regarding child safety.

**Intake Product Vision and Background**

The Legacy System

The CWS/CMS is a 20 year old system with usability, maintenance, and data accuracy issues. The system was originally developed to meets the needs of users to assure the safety, permanency and well-being of children at risk of abuse, neglect or exploitation. CWS is dedicated to modernizing and improving this business functionality. It is used by each of the 58 county child welfare and probation agencies, Title IV-E Tribes, and the State of California. Business function automation will be modernized one module at a time, with modernization including replacing and extending existing functionality.

The Intake Module

Intake Management is the initial entry point into child welfare services and includes processes to receive referrals from community members and mandatory reporters. (Mandatory reporters are individuals, who within their professional capacity—teachers, doctors, etc.—are required by law to report suspicions and/or knowledge of child abuse, neglect, or exploitation).

As one worker stated about the Intake process, “It’s the front door”. And an effective front door leads to a better house.” An effective intake process:

* Allows for quicker and more accurate decisions— which affect the safety of children
* Allows more Referrals to be thoroughly screened in a given day.
* Reduces duplication of Referrals by other workers.
* Reduces the need for Investigators later to reach out to Intake workers in order to clarify case details.
* Helps workers assess incoming abuse situations reports and make informed decisions by providing past case history in a timely and accurate way.

The child welfare worker performing the intake function receives and records information submitted by a Reporting Party who relays information about some form of abuse and neglect. The documentation of this information is considered Creating a Referral. Following the receipt of a referral for child abuse, neglect, or exploitation, child welfare workers screen, assess, and investigate the allegations. This is all recorded within CWS/CMS.

This RFP is only concerned only with **Screening**, **Assessing**, **Creating a Referral** and **Investigations**. Future iterations of the Intake module will solve further workflows or improve upon the ones listed here.

1. **TERM**
2. The term of this Agreement shall commence on ***MM/DD/YYY***, or the date the Agreement is executed by both parties, whichever is later, ***MM/DD/YYYY)*** and continue through ***MM/DD/YYY***.
3. Effective upon approval of the California Department of Technology, Statewide Technology Procurement Divisions (STPD), the term of the Contract is for three (3) month base period with three (3) additional three (3) month terms executed at the State’s sole option.

b. The Contractor shall not be authorized to deliver goods or commence performance of services described in this Agreement prior to the Effective Date. Any delivery of goods or performance of services by the Contractor that is commenced prior to the Effective Date shall be considered gratuitous on the part of the Contractor.

1. **WORK LOCATION**

The Contractor is required to perform all services under this Agreement onsite at the state facility in Sacramento, CA. The CWS-NS *Project* is located at 744 P Street, Sacramento, CA 95814.

1. **COST**

The total cost of this Agreement is **<to be completed at contract award>.** The costs associated with each Fiscal Year are approximate and may be redirected between fiscal years without the requirement of a Contract amendment.

1. **SCOPE OF SERVICES**
2. The Contractor shall provide the following services and artifacts for the development of the Intake module.

**Sprint Zero Artifacts**

1. The Contractor shall produce, review and gain agreement from the State for all Sprint Zero artifacts prior to commencing delivery sprints.
2. The Contractor shall produce a User Story Definition and Acceptance Criteria Format.
3. The Contractor shall produce Coding Standards (including style guidelines) and Commenting Standards, including Peer Review checklist.
4. The Contractor shall produce a Sprint-level Definition of Done that includes the following concepts:
5. Code produced (all ‘to do’ items in code completed)
6. Code commented, checked in and run against current mainline version in source control
7. Peer reviewed (or produced with pair programming) and meeting development standards
8. Builds without errors
9. Unit tests written and passing
10. Deployed to system test environment and passed system tests
11. Passed Product Owner Acceptance Testing
12. Any build/deployment/configuration changes implemented/documented/communicated
13. Relevant documentation produced/updated (e.g., user needs, user stories, sketches, wireframes, clickable prototypes)
14. Remaining hours for task set to zero and task closed
15. The Contractor shall produce a Release-level Definition of Done that includes the following concepts:
16. Release Notes Prepared
17. Deployed to staging environment and integration, performance and load tests run
18. Relevant documentation/diagrams produced and/or updated

**Sprint Planning and Execution**

1. The Contractor shall use an Agile Sprint Planning and User Story Approval process for each Sprint. The Agile Sprint Planning process includes the following activities: Product Backlog refinement, user story creation, estimation and commitment.
2. The Contractor shall demonstrate that each user story has met the definition of done so that the State Product Owner can approve each user story as it is completed.
3. The Contractor shall utilize scrum-based agile processes (e.g., user story development, Product Backlog maintenance, user story user-acceptance, Sprint Retrospective, and Product Review).
4. The Contractor shall revise Sprint Zero artifacts during each Sprint Retrospective process, as appropriate.
5. The Contractor shall generate documentation within the code itself and within the version control system (e.g., through proper use of descriptive commit messages, issue tracking, pull requests, etc.).
6. The Contractor shall use Pivotal Tracker to manage the product backlog, user story acceptance, and maintain a scrum board.
7. The Contractor shall use Slack as the primary mechanism for project-related communication and real-time messaging, archiving and search for all project teams.
8. The Contractor shall provide a report at the conclusion of each sprint that documents the planned user stories, accepted user stories, open impediments, and technical debt.
9. The Contractor shall adhere to Twelve-Factor Application design constraints (see [http://12factor.net/](http:///h)).

**Modularity**

1. The Contractor shall design the application architecture to ensure a separation of concerns and a reasonable degree of modularity between systems.
2. The Contractor shall adhere to the DRY (Don’t Repeat Yourself) principle to ensure that the codebase remains flexible.

**Code Style**

1. The Contractor shall ensure that all code will be written to a language specific code-style guideline (e.g., PEP8 for Python).
2. The Contractor shall use an automated tool to evaluate the codebase and ensure compliance with the code-style guideline (e.g., if the Contractor uses Python, PyLint may be used).

**Version Control System**

1. The Contractor shall manage all assets (e.g., source code, automated tests, user stories, configuration files, knowledge transfer material, etc.) using GitHub.

**Code Review**

1. The Contractor shall ensure all code written by one developer is reviewed by another developer before merging into the mainline codebase.
2. The Contractor shall follow industry standard code review practices (e.g., <http://blog.fogcreek.com/increase-defect-detection-with-our-code-review-checklist-example/>).

**Automated Testing**

1. The Contractor shall create and execute automated unit testing.
2. The Contractor shall create and execute automated system tests to verify all Features of the software module.
3. The Contractor shall create and execute automated Product Owner Acceptance testing to verify all user facing functionality.
4. The Contractor shall run tests automatically on code merge into version control.
5. The Contractor shall use an automated tool that measures the amount of the codebase that is covered by tests (e.g., RCov may be used to measure test coverage of Ruby code).
6. The Contractor shall create and execute automated integration testing with other contractor developed modules.
7. The Contractor shall make the bugs identified during testing available to view real-time and on a historical basis.

**Load Tests**

1. The Contractor shall create and execute load and performance tests at regular intervals, and at each release.
2. The Contractor shall provide a summary of all load and performance test results.

**Accessibility**

1. The Contractor shall incorporate and test accessibility throughout the design and development processes (see section 508 Amendment to the Rehabilitation Act of 1973).
2. The Contractor shall use an automated accessibility testing tool (e.g., Pa11y).

**Issue Tracking**

1. The Contractor shall use GitHub to keep track of all bugs and application issues.

**Mobile Friendly**

1. The Contractor shall design the User Interface (UI) using responsive design.

**Logging and Monitoring**

1. The Contractor shall implement centralized and continuous monitoring.
2. The Contractor shall implement centralized system logging.
3. The Contractor shall implement auditing.

**Security**

1. The Contractor shall use an automated black/white box security scanning tool (e.g., HP Fortify, or [https://hakiri.io](https://hakiri.io/)) to ensure a minimal baseline of security at regular intervals, and at each release.
2. The Contractor shall provide the results of the security scans to the State.
3. The Contractor must adhere to the HTTPS-Only Standard as outlined in <https://https.cio.gov/>.
4. The Contractor shall adhere to the baseline moderate tailored NIST 800-53 (see Attachment).
5. The Contractor shall ensure adequate security controls using penetration testing, red teaming, etc.

## 

## User Authentication

1. The Contractor shall ensure that Intake user authentication and authorization is integrated with the State’s authentication platform.

**Build and Deployment**

1. The Contractor shall provide continuous integration of source code into the source code version control system.
2. The Contractor shall use a continuous source code build tool that enables continuous deployment of all applications into testing and staging environments.
3. The Contractor shall include mock test data that should be publicly accessible for development by other module Contractors and not include personally identifiable information (PII).
4. The Contractor shall use at least one of the following methods to deploy code changes to a staging environment under the control of the Contractor with the issuance of a single command:
5. Containerization (e.g., Docker Engine, Rkt, and Warden)
6. Configuration Management tools (e.g., Chef, Puppet, Salt, and Ansible)
7. The Contractor shall submit server images to State using a Deployment/Release tool at the conclusion of each sprint and upon major releases.
8. The Contractor shall deploy builds to the testing, staging and production environments that will be provided by the State.

**SACWIS and Federal Reporting**

Federal SACWIS requirements mandate functionality within key business practice areas, but allow states some flexibility in how to implement the functions. For example, the federal Administration for Children and Families (ACF) provides specific quality assurance guidelines but allows states latitude with regard to how they ensure completeness, accuracy, and consistency of critical data. The ACF also leaves room for states to identify state-specific business functionality and requirements. As a result of interfaces, the implementation of more flexible modern technologies, and increased reporting abilities, California will better meet federal standards and reporting needs.

1. That Contractor shall ensure that the functionality developed for the Intake module results in compliance with federal Statewide Automated Child Welfare Information System (SACWIS) requirements/.
2. The Contractor shall ensure that the functionality developed for the Intake module supports the federal reporting requirements (e.g., Adoption and Foster Care Analysis and Reporting System and National Child Abuse and Neglect Data System).

Additional information regarding SACWIS is located in the Statewide and Tribal Automated Child Welfare Information Systems – S/TACWIS Review Instrument, located in the Bidders’ Library.

**Intake Scope of Work**

The required approach is to execute the work in phases that can occur during the base or any of the optional periods. The first phase is to support the Search and Referral processes. The second phase is to support the Investigation process.

**Phase 1**

The goal of Phase 1 is to develop the Search and Referral functionality of the Intake Module. This requires the Contractor to research, design, and create a web application that enables the child welfare worker to efficiently perform the following:

* Search previous histories related to the child or related parties
* Make accurate, informed and timely decisions to determine whether an Investigation is required
* Create a Referral based on information captured from a Reporting Party, or other relevant sources;
* Route the referral for investigation or differential response or indicate why no Referral was made

**Discovery/User Research/Design**

1. The Contractor shall conduct user research and supply design services in order to provide user-centered design solutions.

**Understand Business and User Needs (Discovery)**

1. The Contractor shall discover and synthesize the user constraints, opportunities and needs.

The following activities may be necessary to achieve this objective:

* Stakeholder and user interviews
* Contextual inquiry to augment talk-based interview methods
* Usage analysis of existing performance monitoring systems
* User role and task analysis
* Creating personas, scenarios, journey maps, and other artifacts to capture, share, internalize and externalize learnings

**Establish Design Solutions**

1. The Contractor shall provide design solutions for information architecture, workflows, pattern libraries, language, visual design, and overall system performance, and upcoming functionality as prioritized by the Service Manager.

The following activities may be necessary to achieve this objective:

* Develop new information architecture and navigation strategy
* Develop sketches, wireframes, clickable prototypes, final feeling “mock-ups”
* Conduct impromptu and/or frequently scheduled “design spikes” with developers to implement solutions in a low documentation, highly agile way
* Perform QA of user story acceptance criteria
* Conduct usability testing of design solutions

**Develop User Stories for Product Backlog**

1. The Contractor shall turn needs into user stories for the product backlog, which shall be prioritized according to the Service Manager. At this time, Mississippi as started their backlog which is as follows:

The following activities may be necessary to achieve this objective:

* Collaborate with Stakeholders and Service Manager during Product Roadmap planning meetings
* Run iteration planning meetings, daily standups, and retrospectives

**Design a “Joyful” and Modifiable Front-End User Interface**

1. The Contractor shall develop a modern-build front end User Interface (UI) based on a designed or incorporated pattern library that can be modified with relative ease.

The following activities may be necessary to achieve this objective:

* Design and development team work together to create a pattern library
* Conduct a “design sprint” with developers to fine-tune component appearance and behaviors during sprints
* Assist in QA and acceptance of changes on a User Story basis

**Conduct User Research to Continuously Validate Design**

1. The Contractor shall conduct frequent and regular user research releases with primary users to validate quality and direction of design decisions as the Intake module progresses.

The following activities may be necessary to achieve this objective:

* Draft interview scripts
* Travel to conduct on-site, task-based usability tests
* Conduct tests remotely
* Synthesize results and share them with the rest of development, product, and design teams to prioritize improvements

**Phase 2 - Investigation**

The goal of Phase 2 is to develop the Investigation functionality of the Intake Module.

In the course of an investigation, child welfare worker collects information through in-person contacts with the child and family, and individuals who may have information about the events related to allegations in the referral. A child welfare worker assesses safety and risk with both the child and family to determine if the child is safe in their current living environment or at risk for future maltreatment, to identify risk factors and/or to identify appropriate services that may improve the family’s situation.

Background information regarding the alleged perpetrators and any adults residing in the home is collected to determine the risk or safety of the child. Throughout the investigation, all contacts and assessments are documented. The child welfare worker uses the information gathered to help substantiate or invalidate reported allegations. The results of the referral investigation are used to clarify, supplement, and support decisions and actions that the worker takes to support the client and family needs. Response time to investigate a referral can range from immediate (within 24 hours, by regulation) to up to 10 days. Depending on the circumstances of the reported abuse the investigation may include the child welfare worker, staff from a community based organization or licensing organization.

As part of the investigation, the child welfare worker determines whether each allegation is substantiated, inconclusive, or unfounded. The worker will conclude the investigation with a recommendation to close the referral, refer the family to a community based organization for services, open a case for services, or make case management decisions if the case is already open. The worker will record a narrative of the investigation process, document outcomes of the investigation to satisfy all state and federal reporting requirements, submit to an approver for report closure, and notify the mandated reporter of the outcome of the referrals investigation.

Substantiated allegations of physical abuse, emotional abuse, sexual abuse, severe neglect, or exploitation, require the worker to submit a cross report to the California Department of Justice (DOJ) to advise of the outcome and provide details related to the perpetrator and victim(s) in addition to notifying the perpetrator of the report to DOJ. If, during the course of the investigation, the child welfare worker discovers that the home is licensed, the worker will also cross report to CCLD or co-investigate.

1. The Contractor shall develop Investigation functionality that allows authorized users to conduct an investigation after a referral has been made, and fully document the investigator’s activities, assessments, evidence, and findings.
2. The Contractor shall develop Investigation functionality that allows authorized users to generate an electronic report of findings to mandatory reporters.
3. The Contractor shall develop Investigation functionality that allows authorized users to generate a Cross Report.

User stories:

These user needs shall be met in order to fulfill the objectives for performance of this task order, and may be refined by later sprints to continuously meet user needs. User needs are prioritized based on need here in a

Alerts:

As a user, I want the system to assign the intake to the correct county based on the address give so that the intake will be routed to the correct intake supervisor

As a user, I need the system to alert (remind) me to go back to finish partially completed work so that I complete work in a timely manner.

Screening:

As a user, I want the system to determine the priority level based on the information I entered into the system  so that the priority levels are uniform across the state.

As a supervisor, I want the ability to request an override for an assigned screening level from my Regional Director so that special cases can be handled as required.

Web-based reporting tool:

As a user I want the ability to export data from the system so that a report can be created quickly for data purposes.

Duplicates:

As a user, I want the option to import data from a historic intake report so that I save time and reduce redundancy.

As a user, I want the ability to group multiple reports about the same incident, so I can complete multiple reports as one investigation.

Correction Options:

As a person who created a report or another authorized user, I want the option to make corrections so data reporting is more accurate and deadlines will be met.

Intake Narrative:

As a user entering an intake, I want a textbox to record all information provided by the reporter so that all information is captured.  **Acceptance criteria**: unlimited-sized text box; auto-spell/ grammar check

Demographics:

As a user, I want to be able to enter demographic information for a person, so that the information is available for future use.

As a user, I want the system to copy common demographic information to applicable members of the record (e.g., persons in the same household) so that I save time and reduce errors.

Unique ID:

As a user, I want the system to automatically assign a globally unique identifier to each intake so that we can easily distinguish between records.  **Acceptance criteria**: human-friendly (e.g., alphanumeric)

Restricted Access:

As an MDCPS employee, I want to be able to restrict access to an ANE report when it involves an MDCPS employee or high profile person so that confidentiality is protected.

MCI Staff/County staff entering intakes:

As an authorized user, I want to be able to enter an intake report so that I can capture all information.

Multiple allegations, history:

As a user, I want to be able to record details regarding multiple allegations and view a history of anyone involved so I can make a better-informed decision about what I need to do next (e.g., take law enforcement along).

Intake type:

As a user, I want to be able to choose an intake type so that the supervisor and caseworker are aware of the priority and next steps based on intake type.

Access to GPS for investigations

\*\*As a user who needs to visit a site, I want to be able to get directions onto my device to where I need to go so I can get there quickly.

AFCARS and NCANDS requirements:

As a user, I want the system to alert me to collect data so that AFCARS and NCANDS (federal reporting requirements) are met.

Automated assignment:

As a user, I want the system to automatically assign the intake report to the correct county or special investigation unit so I don’t have to determine this.

Person management

As an authorized user, I want to be able to create new or update existing persons at any time with context information so I have information for case management purposes.

Special investigations

As a user, I want the system to assign special investigations to the Special Investigations Unit so that they are assigned to the correct user (role).

Autofill:

As a user, when I fill out a form, I want the system to autopopulate any data it already has so that I avoid errors and save time.

Missing areas:  entry of the intake, each type of intake (what happens), special circumstances around each type

1. **Deliverables and Due Dates**

The deliverables and due dates for this Contract are as follows.

|  |  |  |
| --- | --- | --- |
| **Deliverable** | **Deliverable Description** | **Due Date** |
|  |  |  |
| Sprint Status Report | Identifies the planned user stories, accepted user stories, open impediments, and newly accumulated or resolved technical debt. | Conclusion of each sprint |

1. **PERSONNEL AND RATES**

The personnel shall perform the tasks described in this SOW, at the rates indicated in the Agreement.

1) Given the size, scope, and complexity of this project, it is of utmost importance that the individual(s) have adequate hours to work effectively on this Project. The Contractor shall be responsible for monitoring the monthly hours billed to ensure the individual(s) effectively meet(s) the needs of the Project.

2) The assigned individual(s) will perform the tasks described in this SOW, at the rates indicated in Attachment IV-A, Cost Worksheet. The Contractor shall identify each individual by name, labor category, and hourly rate.

3) Contractor shall provide an Organization Chart identifying each of the proposed team members. Refer to Attachment III-B, Vendor Organization Chart.

**KEY PERSONNEL**

The key personnel specified in this contract are considered to be essential to work performance. At least 15 calendar days before changing any identified individual to other programs or contracts (or as soon as possible, if an individual must be replaced, for example, as a result of leaving the employ of Contractor), Contractor shall notify the State Project Director and shall submit comprehensive justification for the diversion or replacement request (including proposed substitutions for key personnel) to permit evaluation by the State of the effect on performance under this contract. Contractor shall not divert or otherwise replace any key personnel without the written consent of the State Project Manager.

The State may modify the contract to add or delete key personnel at the request of the Contractor or State.

1. The Contractor agrees that the key personnel shall not be removed from the contract effort, replaced or added to the contract without a compelling reason and without compliance with paragraph (2) hereof. The State will not approve substitutions for the sole convenience of Contractor.
2. If any change to the key personnel position becomes necessary (substitutions or additions), the Contractor shall immediately notify the State Project Director in writing, accompanied by the resume of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently approved for that category.
3. All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change.
4. The State reserves the right to have the contractor to replace staff at any time, such right will not be exercised unreasonably. The State will notify the Contractor in writing when exercising that right, and will provide the Contractor with the reason for requiring the replacement. In this event, the Contractor must provide a proposed replacement in accordance with the process and deadline specified herein.
5. **CONTRACTOR STAFF ROLES, RESPONSIBILITIES AND MANDATORY QUALIFICATIONS**

The Contractor shall meet the roles, responsibilities and MQs listed below. All experience used to meet the MQs shall have been where the Contractor had primary responsibility. Refer to Firm Experience Table, Attachment II-F

|  |  |  |
| --- | --- | --- |
| **ROLE** | **RESPONSIBILITY** | **MANDATORY QUALIFICATIONS** |
| Management Lead/Account Representative | The Contractor shall provide a Management Lead. A Management Lead shall ensure that all work on this contract complies with contract terms and conditions and shall have access to vendor’s corporate senior leadership when necessary. The vendor’s management lead shall be the primary interface with the Contract Manager and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by the technical architect when necessary. | 1. The Management Lead shall have been responsible for the management of a system similar in scope to the Bidder’s proposed solution. 2. The Management Lead shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution. 3. The Management Lead shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience. |
| Lead Developer | The Contractor shall provide a Lead Developer.  A Lead Developer is primarily responsible for the architecture and design of the subsystems within the Agile Team’s purview, subject to approval by the Product Owner. The Lead Developer is responsible for choosing the direction of the Agile Team to execute the Product Owner’s vision and goals, and to deliver working software at the end of a sprint. The Lead Developer also helps develop product roadmaps, backlogs, and measurable success criteria, and writing user stories (i.e., can establish a path to delivery for breaking down stories). | 1. The Lead Developer shall have been responsible for the development of a system similar in scope to the Bidder’s proposed solution. 2. The Lead Developer shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution. 3. The Lead Developer shall have a minimum of three years of management experience with software development, design, and the System Development Life Cycle (SDLC) methodologies proposed by the Bidder. 4. The Lead Developer shall have a computer science, engineering, or technology-related baccalaureate degree from an accredited college or university, or commensurate experience. |
| Scrum Master | The Contractor shall provide a Scrum Master.  A Scrum Master is primarily responsible to help the team achieve its goals.  The Scrum Master assures that the team follows the rules of Scrum, helps the team meet their daily and iteration objectives, works to remove impediments in the organization, helps manage the team's relationships with outside stakeholders and facilitates team continuous improvement, and coordinates solution implementation and delivery with other Scrum Masters on the Release train.  The Scrum Master should have experience serving as the client’s point of contact. | 1. The Scrum Master shall have been responsible for the management of a system similar in scope to the Bidder’s proposed solution. 2. The Scrum Master shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution. 3. The Scrum Master shall hold a certification related to Scrum. 4. The Scrum Master shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience. |
| Interaction Designer /  User Researcher /  Usability Tester Team | The Contractor shall provide an Interaction Designer / User Researcher / Usability Tester Team that consists of 2-3 members. The Interaction Designer / User Researcher / Usability Tester Team shall be a cross-functional team consisting of: product identification and research; user behaviors, needs, and motivations; testing metrics and narrative. | 1. Each member of the Interaction Designer / User Researcher / Usability Tester Team shall have been involved in at least two software development projects similar in scope to the Bidder’s proposed solution. 2. Each member of the Interaction Designer / User Researcher / Usability Tester Team shall have been involved in at least one agile software development project. 3. Each member of the Interaction Designer / User Researcher / Usability Tester Team shall have at least 2 years experience in at least one of the following, and between all team members each of the following must be covered: 4. Planning and leading user research 5. User interviews 6. Planning and leading 1:1 task based usability testing 7. Presenting synthesis to clients |
| Product Development Team | The Contractor shall provide a Product Development Team that consists of 3-5 members. The Intake Product Team shall be a cross-functional team consisting of: developers, UX/UI designers, visual designers, content strategists/writers, functional experts, etc., as appropriate for the sprint and module. | 1. Each member of the Product Development Team shall have been involved in at least two software development projects similar in scope to the Bidder’s proposed solution. 2. Each member of the Product Development Team shall have been involved in at least one agile software development project. 3. Each member of the Product Development Team shall have at least 2 years experience in at least one of the following, and between all team members each of the following must be covered: 4. Writing the back-ends of modern web applications (e.g. using frameworks such as Ruby on Rails, Flask, or Express) 5. Writing the front-ends of modern web applications (e.g. using a modern Javascript front-end framework such as React, Ember, or Backbone; using modern, web standards-compliant CSS and HTML) 6. Secure REST APIs 7. Enterprise user authentication tools 8. Modern security, monitoring, and logging practices for system administration 9. Modular web application development 10. Test-driven development 11. Automated unit and integration testing 12. Automated acceptance testing 13. Continuous build processes and tools 14. SQL and SQL optimization 15. Load and Performance testing 16. Security and system administration 17. Modern continuous monitoring tools 18. NIST 800-53 controls 19. Penetration testing |

**STATE ROLES**

|  |  |
| --- | --- |
| **ROLE** | **RESPONSIBILITY** |
| Product Owner | The State will provide one Product Owner. The Product Owner is an empowered individual who will interface with the client’s stakeholders, synthesize feedback, and make decisions on the product’s priorities and scope. The Product Owner, working with stakeholder interests, user needs, and insight from the product team, will establish the vision and goals for the Child Welfare System INTAKE and prioritize user stories to include in sprints and strategize release cycles. |
| Project Manager | The State will provide one Project Manager. The Project Manager will manage the daily and iteration objectives, work to remove impediments in the organization, help manage the team's relationships and facilitate team continuous improvement, and coordinates solution implementation and delivery with the Scrum Master(s). |
| Performance Analyst | The State will provide one Performance Analyst. The Performance Analyst will specify, collect and present key performance data and analysis of the product. |
| Technical Architect | The State will provide one Technical Architect. The Technical Architect will be responsible for translating the requirements into the architecture and describing/managing it through the set of architecture and design artifacts to provide the overall technical vision. |

1. **PAYMENTS AND INVOICING**

Payment for services performed under this Agreement shall be made in accordance with the State of California’s Prompt Payment Act (GC Section 927 et seq.).

**Submission of Invoices**

1. Payment shall be made after the completion and acceptance for two sprints (i.e. every four weeks). Invoices shall be submitted after completion and acceptance of two sprints. All invoices shall be submitted in triplicate, detailing the labor category hours (incremental hours shall be billed to the nearest 15 or 30 minutes) and dollars and include the following:
2. Transmittal with the Agreement number;
3. A certification statement signed by a company official, attesting to the accuracy of the invoice data; and
4. Copies of signed timesheet(s);
5. Invoices shall be submitted directly to:

**Office of Systems Integration**

**Attn: Accounting Office**

**2525 Natomas Park Drive, Suite 200**

**Sacramento, CA 95833**

**Payment Method**

Payment to the Contractor will be made on a time and materials basis per the hourly labor classifications set forth in the Contract. The payment amount for each sprint is capped at a total of each resource’s labor classification rate multiplied by 90 hours. A sprint is defined as a two (2) week period.

**Payment Frequency**

Payment shall be made after the completion and acceptance for two sprints (i.e. every four weeks).

**Payment Withhold**

To ensure satisfactory performance by the Contractor and mitigate risk to the State, the State will withhold ten (10) percent from each payment. The State will release the Withhold payment to the Contractor at the conclusion of the entire Contract, provided that all accepted user stories have achieved the Release-level Definition of Done.

**Travel and Reimbursement**

The State has included a travel budget included in the cost of this Agreement. The State shall reimburse the Contractor for State pre-approved and required consultant travel mileage, lodging, and per diem costs up to the maximum allowed and in accordance with the guidelines currently in effect, as established by the California Department of Human Resources (CalHR), for excluded employees. If the CalHR rates change during the term of the Agreement, the new rates shall apply upon their effective date and no amendment to this Agreement shall be necessary.

Travel invoices shall be submitted monthly, in arrears. All invoices shall be submitted in triplicate, detailing travel expenses in accordance with CalHR rates and include the following:

* 1. Transmittal with the Contract number,
  2. A certification statement signed by a company official, attesting to the accuracy of the invoice data,
  3. Supporting documentation, receipts and explanations including the individual’s name, detailed project description, and hours/mileage; and
  4. Invoices shall be submitted directly to the address listed above in Paragraph 9.a.2

1. **POINTS OF CONTACT**

|  |  |
| --- | --- |
| **Contractor – Contract Manager**: | |
| Name, Title: | ***[To be completed upon agreement award.]*** |
| Address: |  |
| Telephone Number: |  |
| Fax Number: |  |
| E-mail address: |  |

|  |  |
| --- | --- |
| **State – Contract Manager:** | |
| Name | ***Robyn Sasaki*** |
| Address: | 744 P Street, 12thFloor – OB 9, MS9-12-83 |
| Telephone Number: | (916) 654 -0600 |
| Fax Number: |  |
| E-mail address: | Robyn.Sasaki@osi.ca.gov |

1. **STATE FURNISHED ITEMS**

The following items shall be provided by the State to support this effort:

* 1. Office work space for the duration of the Agreement includes desk, chair, desk phone, and Internet connection.
  2. Access to office building and office suite.
  3. All policies and procedures regarding access to and the use of the state facilities are applicable.
  4. Collaboration, version control, and agile project management software services.
  5. Integration, Training, Staging and Production Environments.

1. **CONTRACTOR FURNISHED ITEMS**
2. Contractor to provide primary computer workstation (desktop or laptop).
3. Contractor to provide development and system test environments at no cost to the State.
4. **RESPONSIBILITIES OF PARTIES**
5. **Contractor Responsibilities**
   * + 1. All work products and deliverables shall be stored on the State document repository (e.g. GitHub, Slack) in a format compatible with OSI document standards. The most current version of all work products and deliverables shall be continuously available for State review at all times.
       2. The Contractor shall receive all project communications and has the authority to act on all aspects of the services. This person will review the Agreement and associated Agreement documents with the State Contract Manager to ensure understanding of the responsibilities of both parties.
       3. Prior to expiration of the Agreement, the Contractor shall return all State property, including security badges to the State Contract Manager.
       4. As part of this Agreement, the Contractor (data custodian) shall be responsible for all costs incurred by the State (data owner) due to any and every security incident resulting from the Contractor’s failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. If the Contractor experiences an actual or potential loss of data or breach of data security, the Contractor shall, within two (2) hours of its discovery thereof, report the loss or security breach to the OSI Information Security Officer at osiinfosecurity@osi.ca.gov. If the State determines that notice to the individual(s) whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the State. These costs include, but are not limited to, consultant time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
       5. The Contractor shall comply with all applicable State policies including, but not limited to (State Administrative Manual 5300-5399, State Information Management Manual procedures, and OSI’s security policies including, but not limited to, it’s Acceptable Use Policy, Confidentiality and Non-Disclosure Policy, CHHS Security Policies and OSI Security templates, which may be found at www.osi.ca.gov. (See Attachment III-F, Special Provisions.)
       6. All Contractor-owned or managed laptops, Ultra books, net books, tablets, Smart phones and similar devices, if allowed by the State Contractor Manager, shall be encrypted using commercial third-party encryption software. The encryption software shall meet the level standards of National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules. Additionally, anti-virus, anti-malware software shall be used and kept up to date along with software patches and supported versions. The OSI Information Security Office shall have the right to audit Contractor-owned devices connected to State networks.
       7. If Contractor use of removable media storage devices (i.e. Universal Serial Bus [USB] thumb drives, disk tapes, micro SD, SD cards, CD/DVD, etc.) is allowed by the State Contract Manager, all electronic files stored on the removable media storage device used to store State information shall be encrypted using a commercial third-party encryption software. The encryption software shall meet the standards set forth in NIST FIPS 140-2. Information stored on approved removable storage devices shall not be copied to any unencrypted computer (i.e., desktop or laptop) not connected to State network. Any personally identifiable information, personal health information, or other confidential information shall be encrypted when stored on State network file shares or document repositories.
6. **State Responsibilities**
   1. The State Product Owner will provide product vision, prioritization and User Story acceptance.
   2. The State Project Director shall receive all project communications and has the authority to act on all aspects of the services. This person will review the Agreement and associated Agreement documents with the Contractor to ensure understanding of the responsibilities of both parties.
   3. The State will provide timely review and approval of the information and documentation provided in order for the Contractor to perform its obligations under this Agreement.
   4. The State will provide the following software tools: Slack, Pivotal Tracker, and GitHub.

**ATTACHMENT 1**

**SPECIAL PROVISIONS**

**ATTACHMENT 2**

**DEFINITIONS**

**ATTACHMENT 3**

**NIST 800-53 OPERATIONAL**

**ATTACHMENT 4**

**NIST 800-53TECHNICAL**

**ATTACHMENT 5**

**Contractor Sprint Status Report**

***[Sample]***

**[Insert page 1 of #]**

For [insert reporting period -- month and year]

|  |  |
| --- | --- |
| **Contractor:** | [Company Name] |
| **Agreement #:** | [Project Agreement Number] |
| **Title:** | [Project Title] |

*[This sample template describes the required contents of the Contractor’s monthly status report.]*

# 1 Introduction

*[A brief overview of the activity completed.]*

# 2. Activity Summary

*[This section shall contain the information listed below. Planned user stories and accepted user stories.]*

# 3. Open Impediments.

*[Impediments that were not resolved during the sprint.]*

# 4. Technical Debt.

*[New accumulated technical debt and resolved technical debt during the sprint.]*

**ATTACHMENT 6**

**Contractor Status Report**

***[Sample]***

**[Insert page 1 of #]**

For [insert reporting period -- month and year]

**Deliverables this Month** -- *[Show any deliverables that were provided, or should have been provided, during the month. For example, the monthly report for June would probably list the report for May that was delivered in June. Overdue or late deliverables require an explanation.]*

**Table 1. Deliverables this Month**

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable Title** | **SOW Reference** | **Date Due** | **Date Delivered** |
| [Deliverable title, from SOW requirement] | [Reference, as used in SOW; i.e., task number or unique reference] | [SOW due date] | [Actual delivery date] |
|  |  |  |  |
|  |  |  |  |

## Deliverables Status - [List all of the deliverables from the SOW, with current status. Each deliverable, whether delivered or due, should be shown. Periodic deliverables do not need to be listed more than once—see example. Other, ad-hoc deliverables should also be listed. These items should also be tied to the SOW paragraph that the tasking fell under.]

**Table 2. Deliverables Status**

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable Title** | **SOW Reference** | **Date Due** | **Date Delivered** |
| [Deliverable title, from SOW requirement] | [Reference, as used in SOW; i.e., task number, or unique reference] | [SOW due date] | [Actual delivery date] |
| Monthly Report | [Example: Task 1.2 – Status Report | Monthly | Monthly |

# **Concerns/Issues** -- *[List any concerns or issues that are pertinent to completion of the SOW tasks. If there are no concerns or issues, please indicate by a statement such as “None at this time.”]*

# **Financial Summary** -- *[Show the task’s costs vs. the expenditure plan as presented in the TAP. If no TAP was submitted for your tasking, the status should still be shown against anticipated expenditures.]*

[Any significant variance (greater than ten (10) percent, or as stated in the contractor’s SOW) should be explained in the comment column. Variance is defined as “Actual-Budgeted”.]

**Signed by Contractor Contract Manager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_**

**Approved/Signed by State Contract Manager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | ATTACHMENT 7  ADD, DELETE OR SUBSTITUTE  CONTRACTOR PERSONNEL REQUEST FORM | | | | | | |
| **Contractor Name** | | | | | **Contractor Phone No.** | | Date | |
| **Project Name/Agreement Number** | | | | | | | | |
| **Personnel To Be Added** | | **Personnel Replaced** | | | **Proposed Effective Date** | **Classification** | | **Resume Meets MQs and requirements** |
|  | |  | | |  |  | | **☐** |
| **Personnel To Be Deleted** | | **Date Effective** | **Reason** | | | | | |
|  | |  | **Reason:** | | | | | |
| **Comments/Special Instructions**  **Please note:**  **The changes as indicated in this request are being made at no additional cost to the STATE. – Sample**  **(*Include this language, if applicable).*** | | | | | | | | |
| **STATE Acceptance** | | | | **Contractor Acceptance** | | | | |
| **Division/Project** | | | | **Contractor** (If other than an individual, state whether a corporation, partnership, etc.) | | | | |
| **By (Authorized Signature)** | | | | **By (Authorized Signature)** | | | | |
| **Printed Name of Person Signing** | | | | **Printed Name of Person Signing** | | | | |
| **Title** | | | | **Title** | | | | |

**ATTACHMENT 8**

**OSI Special Provisions**

Special Provisions shall include any special directions or project specific requirements that are not otherwise stated explicitly in the agreement.

* + - * 1. **OSI SECURITY**

Information Confidentiality and Security Requirements for Leveraged Procurements

1. **Definitions***.* For purposes of this Exhibit, the following definitions shall apply:
2. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6270) or other applicable state or federal laws.
3. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6270) or other applicable state or federal laws.
4. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.
5. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. **It is OSI’s policy to consider all information about individuals private unless such information is determined to be a public record.** This information shall be protected from inappropriate access, use, or disclosure and shall be made accessible to data subjects upon request. Personal Information includes the following:

Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

1. **Nondisclosure**. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).
2. The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.
3. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the OSI State Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.
4. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than OSI without prior written authorization from the OSI State Contract Manager, except if disclosure is required by State or Federal law.
5. The Contractor shall observe the following requirements:
6. **Requirements and Guidelines**.
7. The Contractor shall classify their data pursuant to the California State Administrative Manual (SAM) 5305.5.
8. The Contractor shall comply with the following:
   * 1. The California Information Practices Act (Civil Code Sections 1798 et seq.);
     2. Security provisions of the SAM (Chapters 5100 and 5300) and the California Statewide Information Management Manual (SIMM) (Sections 58-C, 58-D, 66-B, 5305-A, 5310-A and B, 5325-A and B, 5330-A, B and C, 5340-A, B and C, 5360B);
     3. Privacy provisions of the Federal Privacy Act of 1974;
9. The Contractor shall comply with the information security and privacy controls set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP); including but not limited to NIST 800-53R4 (tailored to OSI Requirements for a Low or Moderate Level Of Concern).
10. **Safeguards**. The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of personal, sensitive, and confidential information (PSCI), including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of OSI. The Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor’s operations and the appropriate levels of security (confidentiality, integrity, and availability) for the data based on data categorization and classification and FIPS Publication 199 protection levels, Including at a minimum the following safeguards:
11. **Personnel Controls**
12. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of OSI, or access or disclose OSI Protected Health Information (PHI) or Personally Identifiable Information (PII) shall complete information privacy and security training, at least annually, at the Contractor’s expense. Each workforce member who receives information privacy and security training shall sign a certification, indicating the member’s name and the date on which the training was completed. These certifications shall be retained for a period of six (6) years following agreement termination.
13. ***Employee Discipline.*** Appropriate sanctions shall be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
14. ***Confidentiality Statement.*** All persons that will be working with OSI PSCI shall sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to OSI PSCI. The statement shall be renewed annually. The Contractor shall retain each person’s written confidentiality statement for OSI inspection for a period of three (3) years following agreement termination.
15. ***Background Check.*** Before a member of the Contractor’s workforce may access OSI PSCI, the Contractor shall conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member’s background check documentation for a period of three (3) years following agreement termination.
16. **Technical Security Controls**
17. **Workstation/Laptop Encryption.**All workstations and laptops that process and/or store OSI PSCI shall be encrypted with an OSI approved solution (i.e. FIPS 140-2). The encryption solution shall be full disk.
18. **Minimum Necessary**. Only the minimum necessary amount of OSI PSCI may be downloaded to a laptop or hard drive when absolutely necessary for current business purposes.
19. **Removable Media Devices**. All electronic files that contain PSCI data shall be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) with an OSI approved solution (i.e. FIPS 140-2).
20. **Email Security**. All emails that include OSI PSCI shall be sent in an encrypted method using an OSI approved solution.
21. **Antivirus Software**. All workstations, laptops, other devices, and systems that process and/or store OSI PSCI shall have a commercial third-party anti-virus software solution with a minimum daily automatic update.
22. **Patch Management**. All workstations, laptops, other devices, and systems that process and/or store OSI PSCI shall have security patches applied and up-to-date.
23. **User IDs and Password Controls**. All users shall be issued a unique user name for accessing OSI PSCI. Passwords shall not to be shared. Passwords shall adhere to the following:

* Be at least eight characters
* Be a non-dictionary word
* Not be stored in readable format on the computer
* Be changed every 90 days
* Be changed if revealed or compromised

Password shall be composed of characters from at least three of the following four groups from the standard keyboard:

* Upper case letters (A-Z)
* Lower case letters (a-z)
* Arabic numerals (0-9)
* Non-alphanumeric characters (punctuation symbols)

1. **Data Destruction**. The Contractor shall meet the standards as set forth in NIST800-88 for destruction of data. All OSI PSCI shall be wiped from systems when the data is no longer necessary. The wipe method shall conform to Department of Defense standards for data destruction. If data was PII or PHI, then the Gutmann 35 pass wipe is required. All OSI PSCI on removable media shall be returned to OSI when the data is no longer necessary. Once data has been destroyed and logged, the OSI State Contract Manager shall be notified and provided logs for auditing and retention period.
2. **Remote Access**. Any remote access to OSI PSCI shall be executed over an encrypted method approved by OSI. All remote access shall be limited to minimum necessary and least privilege principles. Remote Access shall meet security standards as defined in SAM 5360.1 and SIMM 5360-A.
3. **System Security Controls**
4. ***System Timeout.*** The System shall provide an automatic timeout after no more than 20 minutes of inactivity.
5. ***Warning Banners.*** All Systems containing OSI PSCI shall display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users shall be directed to log off the system if they do not agree with these requirements.
6. ***System Logging.*** The System shall log successes and failures of user authentication at all layers. The System shall log all system administrator/developer access and changes if the system is processing and/or storing PSCI. The System shall log all user transactions at the database layer if processing and/or storing OSI PSCI.
7. ***Access Controls.*** The System shall use role based access controls for all user authentications, enforcing the principle of least privilege.
8. ***Transmission Encryption.*** Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A. All data transmissions shall be encrypted end-to-end using an OSI approved solution, when transmitting OSI PSCI. See the CHHS Security Policy – Data Encryption at the following link: [CHHSA Security Policy Data Encryption](http://osiintranet.osi.ca.gov/LinkClick.aspx?link=CS%2fCS_InfoSec%2fPolicies%2fCHHSA+Security+Policy+Data+Encryption+2014.pdf&tabid=284&mid=964)
9. ***Host Based Intrusion Detection.*** All systems that are accessible via the Internet or store OSI PSCI shall actively use a comprehensive third-party real-time host based intrusion detection and prevention solution.
10. ***System Security Review***
11. The Contractor shall obtain independent security risk assessment consultants to meet the SAM 5305.7 and NIST standards (800-30, 800-37, 800-39, and 800-53) as well as OWASP standards including but not limited to the Development and Testing Guidelines for web services. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not:

* Create a mutual or conflicting interest with the organizations where the assessments are being conducted.
* Self-assess their work.
* Act as management or employees of the organizations they are serving.
* Place themselves in advocacy positions for the organizations acquiring their services.
* Have an affiliation, either personal or business, with the Contractor or subcontractors working under contract with the OSI.

1. The OSI shall have approval of the independent risk assessment consultants that will perform the security risk assessments prior to the Contractor hiring the firm.
2. The independent security risk assessment firm shall have references from comparable State agencies (comparable system complexity as OSI).
3. The Contractor shall have independent security risk assessment consultants conduct security risk assessments every two years of the OSI Project Systems (e.g. CWS/CMS, CWS-NS, CMIPS II, and SFIS) and Project Support Systems (.e.g. shared drives, web sites, web applications, Clarity, Sharepoint, County Access Data, and SARS).
4. The Contractor shall have the security risk assessment provide a gap analysis using the latest version of the Low or Moderate Tailored Baseline NIST 800-53 security controls.
5. The State Project Manager or designee and the OSI ISO shall have full access to the results of the independent risk assessment.
6. The Contractor shall provide to the OSI a Security Assessment Report created by the independent security assessors as defined in NIST 800-53. This report shall contain, as a minimum, identification and score of risks and provide recommended mitigation solutions.
7. **Audit Controls**
8. ***Log Reviews.*** All systems processing and/or storing OSI PSCI shall have a routine procedure in place to review system logs for unauthorized access.
9. ***Change Control.*** All systems processing and/or storing OSI PSCI shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.
10. **Business Continuity / Disaster Recovery Controls**
11. ***Emergency Mode Operation Plan.*** The Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic OSI PSCI in the event of an emergency. An emergency is an interruption of business operations for more than 24 hours.
12. ***Data Backup Plan.*** The Contractor shall have established documented procedures to backup OSI PSCI to maintain retrievable exact copies of OSI PSCI. The plan shall include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore OSI PSCI should it be lost. At a minimum, the schedule shall be a weekly full backup and monthly offsite storage of OSI data.
13. **Paper Document Controls**
14. ***Supervision of Data.*** OSI PSCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, or desk. Unattended means that information is not being observed by an employee authorized to access the information. OSI PSCI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
15. ***Escorting Visitors.*** Visitors to areas where OSI PSCI is contained shall be escorted and OSI PSCI shall be kept out of sight while visitors are in the area.
16. ***Confidential Destruction.*** The Contractor shall meet the standards as set forth in NIST 800-88 for destruction of data. OSI PSCI shall be disposed of through confidential means, such as cross cut shredding and pulverizing.
17. ***Removal of Data.*** OSI PSCI shall not be removed from the premises of the Contractor except with express written permission of OSI.
18. ***Faxing.*** Faxes containing OSI PSCI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending. Contractor fax machines shall be located in secure areas, per SAM 5365.1.
19. ***Mailing.*** OSI PSCI shall only be mailed using secure methods. Large volume mailings of OSI PSCI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail shall be encrypted with an OSI approved solution.
20. **Physical Transport of Paper/Electronic Data/Media**

There are specific precautions that shall be taken when transporting electronic data/media. The data/media shall be wrapped or sealed in an envelope or pouch in such a manner that the contents cannot be identified during the transportation process. The outside of the container shall clearly identify the addressee, which includes the name, address and telephone number where he/she can be reached. Departments should ensure that transported data/media be delivered only to the appropriate individuals who are authorized to receive the information. This can be accomplished by implementing a tracking method by which the sender and the recipient can sign and verify delivery and receipt of the information.

The Contractor shall ensure that there is a tracking process in place for the transportation of data/media, whether in paper records or physical media devices and that accountability is strongly emphasized with the establishment of this process. Existing tracking processes such as those associated with FedEx, UPS and the U.S. Postal Service are permitted, however when sending information on physical media devices via these methods or by similar means, **the information shall be encrypted**.

1. **California Public Records Act**.The Contractor shall work cooperatively with the State to respond timely and correctly to public records act requests.
2. **Security Officer**. The Contractor shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with OSI.
3. **Training**. The Contractor shall provide training on its data privacy and security policies, at least annually, at its own expense, to all its employees and volunteers who assist in the performance of functions or activities on behalf of OSI under this Agreement and use or disclose PSCI.
4. The Contractor shall require each employee and volunteer who receives data privacy and security training to sign a certification, indicating the employee’s/volunteer’s name and the date on which the training was completed.
5. The Contractor shall retain each employee’s/volunteer’s written certifications for OSI inspection for a period of three years following agreement termination.
6. **Breaches**.
7. **Discovery and Notification of Breach**. The Contractor shall be responsible for facilitating the security incident process as described in California Civil Code 1798.29(e), California Civil Code 1798.82(f), and SAM 5340, Incident Management. The Contractor shall notify OSI immediately by telephone call plus email or fax upon the discovery of breach of security of PSCI in computerized form if the PSCI was, or is reasonably believed to have been, acquired by an unauthorized person, or within two hours by email of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PSCI in violation of this Agreement, this provision, the law, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the OSI Program Contract Manager, the OSI Privacy Officer and the OSI Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PSCI, notification shall be provided by e-mailing the OSI Security Office at [osiinfosecurity@osi.ca.gov](mailto:osiinfosecurity@osi.ca.gov). The Contractor shall take:
8. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
9. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
10. **Investigation of Breach**. The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI and within twelve (12) to twenty-four (24) hours of the discovery, shall notify the OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer of:
11. What data elements were involved and the extent of the data involved in the breach;
12. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PSCI;
13. A description of where the PSCI is believed to have been improperly transmitted, sent, or utilized;
14. A description of the probable causes of the improper use or disclosure; and
15. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.
16. **Updates on Investigation**. The Contractor shall provide regular (every 24 hours) updates on the progress of the investigation to the OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer.
17. **Written Report**. The Contractor shall provide a written report of the investigation to the OSI Program Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer within seven (7) working days of the discovery of the breach or unauthorized use or disclosure. The report will, at a minimum, follow the format of SIMM 5340-B. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.
18. **Notification of Individuals**. The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer shall approve the time, manner and content of any such notifications.
19. **Affect on lower tier transactions**. The terms of this Exhibit shall apply to all agreements, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.
20. **Contact Information**. To direct communications to the above referenced OSI staff, the Contractor shall initiate contact as indicated herein. OSI reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

|  |  |  |
| --- | --- | --- |
| **OSI State Contract Manager** | **OSI Privacy Officer** | **OSI Information Security Officer** |
| See the agreement for State Contract Manager information | Privacy Officer  c/o OSI Legal Division  Office of Systems Integration  2525 Natomas Park Drive, Suite 200  Sacramento, CA 95833  Email: [@osi.ca.gov](mailto:caroline.bolton@osi.ca.gov)  Telephone: (916) 263-0737 | Information Security Officer  OSI Information Security Office  Office of Systems Integration  2525 Natomas Park Drive, Suite 200  Sacramento, CA 95833  Email: [osiinfosecurity@osi.ca.gov](mailto:osiinfosecurity@osi.ca.gov)  Telephone: (916) 263-0744 or  (916) 825-9213 |

1. **Audits and In** Office of Systems Integration **spections**. From time to time, OSI may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. The Contractor shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that OSI inspects, or fails to inspect, or has the right to inspect the Contractor’s facilities, systems and procedures does not relieve the Contractor of its responsibility to comply with this ICSR exhibit.