



CALIFORNIA STATE TEACHERS' RETIREMENT SYSTEM

**Technology Services
California Multiple Award Schedule (CMAS) Agreement
Senior System Engineer**

REQUEST FOR OFFER # 5805139216

**OFFER DUE DATE
September 16, 2026 2:00 P.M.**

Ryan Zelachoski
Technology Services Procurement Analyst
California State Teachers' Retirement Systems
ITProcurement@CalSTRS.com

REQUEST FOR OFFER

You are invited to review and respond to the California State Teachers' Retirement System (CalSTRS), Request for Offer (RFO), entitled Senior System Engineer. Read this document carefully. In submitting your Offer, you must comply with the instructions, terms and conditions stated in this RFO and in your Information Technology CMAS contract.

Offers must be submitted to CalSTRS via email to ITProcurement@CalSTRS.com and must be received by CalSTRS no later than September 16, 2026 by 2:00 P.M., Pacific Time (PT). Offers received after the specified date and time may be rejected.

Respondents requiring clarification of the intent and content of this RFO, or on the competitive process, may request clarification only by submitting written questions to:

Ryan Zelachoski
Technology Services Procurement Analyst
ITProcurement@CalSTRS.com

Refer to Attachment IV, Frequently Asked Questions, prior to submitting any written questions. Any additional questions must be received by September 7, 2026, by 2:00 P.M., PT. Questions received by this date will be answered in writing, without identifying the source of query.

Any attempt by a firm responding to this Offer to initiate contact with any member of the Teachers' Retirement Board and/or CalSTRS staff, other than the CalSTRS contact listed above, regarding this RFO process may disqualify the firm from further consideration.

Please note that no *verbal* information given will be binding upon the California State Teachers' Retirement System unless such information is incorporated into this RFO via an addendum.

TABLE OF CONTENTS

A. INTRODUCTION

B. BACKGROUND

C. QUALIFICATIONS REQUIREMENTS

D. OFFER REQUIREMENTS AND INFORMATION

E. ATTACHMENTS

- I. Information and Offer Sheet
- II. Proposed Project Person Skill Summary Sheet
- III. Proposed Project Person Business Reference Sheet
- IV. Frequently Asked Questions
- V. Statement of Work

F. SAMPLE AGREEMENT

- 1. Agreement Terms and Conditions
- 2. Exhibit A – Statement of Work
- 3. Exhibit B – <Contractor's> Key Personnel
- 4. Exhibit C – Teachers' Retirement Board Governance Manual – Third Party Economic Interest Disclosure Policy
- 5. Exhibit D – Form 600-H Third Party Economic Interest Disclosure
- 6. Exhibit E – Contractor Background Investigation Policy
- 7. Exhibit F – Certification of Contractor's Employee Background Investigation Form
- 8. Exhibit G – Personal History Statement
- 9. Exhibit H – CalSTRS Information Security and Privacy Addendum
- 10. Exhibit I – Confidentiality, Non-Disclosure and Acceptable Use Agreement
- 11. Exhibit J – CalSTRS Minimum Information Security Requirements

GENERAL INFORMATION

A. INTRODUCTION

CalSTRS is the largest educator-only pension fund in the world. CalSTRS administers a hybrid retirement system, consisting of traditional defined benefit, cash balance and voluntary defined contribution plans. CalSTRS also provides disability and survivor benefits. CalSTRS serves California's public school educators and their families from the state's school districts, county offices of education and community college districts. For more information on CalSTRS and its various programs, please refer to the CalSTRS Website at: <https://www.CalSTRS.com>.

The purpose of this RFO is to select one (1) experienced Senior System Engineer with in-depth knowledge and hands-on experience in Software as a Service (SaaS) systems. The ideal candidate should be skilled in implementing, enhancing, configuring, customizing, and validating SaaS solutions. In addition, responsibilities will include providing technical support, resolving defects, building dashboards, managing vendors, and overseeing contract management. This position is expected to work within the Enterprise IT Solutions & Innovation Division. The services required are more fully described in Attachment V, Statement of Work, included in this document.

CalSTRS will only accept one (1) offer per Vendor (Respondent) for this RFO. Each offer shall only include one (1) proposed project person.

The total services period may be up to twelve (12) months, with an option to extend up to twenty-four (24) additional months, at an estimated average of 160 work hours per month at the rate negotiated at contract execution. Any contract resulting from this RFO may be amended to add time or funds, at the sole discretion of CalSTRS.

The Vendor/Contractor must be able to perform all work on-site at the CalSTRS headquarters facility in West Sacramento, CA. At CalSTRS' discretion, a different approach (i.e., fully in-office, fully remote or different work hours) may be utilized based on CalSTRS business need and/or directive. Work must be performed during CalSTRS business hours and shall not be permitted on California State Holidays identified on the California Department of Human Resources website, unless pre-approved in writing by CalSTRS management. All work schedules must be pre-approved in writing by CalSTRS management and must adhere to all applicable CalSTRS policies and procedures. The Vendor/Contractor is responsible for any travel costs (including travel time) that they may incur while providing the services identified in the Statement of Work.

The proposed project person selected as a result of this RFO will be under the direction of the CalSTRS Senior Manager of System and Production Services or designee and may be assigned one or more teams/programs/projects during the services period.

B. BACKGROUND

The CalSTRS Enterprise IT Solutions and Innovation Division provides technical guidance, cloud-based application design and development, software development, system design, and services for the maintenance, enhancement, and integration of existing and new enterprise applications. Application developers lead or participate in cross-functional development and maintenance efforts, governing changes and planning for

continuous improvement of a consistent, shared, and reusable architecture that allows CalSTRS to obtain the optimum value for the investments made in technology.

The System and Production Services team manages multiple SaaS applications, including analysis, onboarding, configuration, customization, enhancements, defect resolution, dashboard creation, and deployment across various environments. These SaaS systems are used throughout CalSTRS by multiple departments for a variety of business purposes.

CalSTRS Enterprise IT Solutions and Innovation Division is seeking a Senior System Engineer with experience in SaaS implementation, configuration, customization, enhancement, validation, support, and building dashboards and reports. Experience with ServiceNow, Salesforce, vendor management, and contract management of SaaS platforms is desired. The ideal candidate will also have experience in solution design, troubleshooting, detailed technical design, development, test automation, and deployment.

For more information about the CalSTRS organization, mission, vision, and strategic and business plans, go to www.CalSTRS.com.

C. QUALIFICATIONS REQUIREMENTS

The proposed project person must meet all of the following minimum qualifications to CalSTRS' satisfaction to be given further consideration. Failure to satisfy any of the minimum qualifications upon submittal of the Offer may result in the immediate rejection of the Offer.

Minimum Administrative Qualifications

As of the Offer Due Date:

1. The Respondent must hold a current Information Technology California Multiple Award Schedule (CMAS) agreement with the California Department of General Services and must comply with the instructions, terms and conditions stated in the Leveraged Procurement Agreement.
2. The Respondent must submit all data/information and attachments requested in the offer format described below under Section D, Subsection 2, Offer Requirements. **Failure to submit Attachment I - Information and Offer Sheet and Attachment II - Proposed Project Person Skill Summary Sheet, by the Offer Due Date, will be grounds for immediate rejection of the submission.**

Minimum Technical Qualifications

As of the Offer Due Date, the proposed project person must have the following listed experience, knowledge, skills and abilities, as evidenced by Attachment II, Proposed Project Person Skill Summary Sheet and resume:

1. A minimum of seven (7) years of experience in Software-as-a-Service (SaaS) application implementation, enhancement, and testing.
2. A minimum of seven (7) years of experience in technical and administrative support of SaaS applications, such as researching technical issues, debugging and resolving issues in a timely manner.
3. A minimum of seven (7) years of experience of onboarding SaaS applications including configuring SaaS systems, generating dashboards and working with the third-party vendors and SaaS clients.

4. A minimum of seven (7) years of experience in Software Development Life Cycle (SDLC) such as analyzing, solutioning, detail design, development, testing, automation and deployment.

Desirable Technical Qualifications

It is **desirable** for the proposed project person to have the following listed experience, knowledge, skills and abilities as evidenced by Attachment II, Proposed Project Person Skill Summary Sheet and resume:

1. A minimum of five (5) years of hands-on coding experience in algorithm and data structures.
2. Experience with technical integration between SaaS solutions and the ServiceNow “Now Platform” including but not limited to Incident Management, Change Management, Service Level Management, and Service Catalogue.
3. Experience in maintaining and administering ServiceNow Information Technology Service Management (ITSM), Information Technology Asset Management (ITAM), and Information Technology Operations Management (ITOM).
4. Extensive experience in using, defining, and generating reports (e.g., status, statistics, analysis) from ServiceNow for communication and periodic reporting of SaaS applications and solutions across the enterprise.
5. Experience with AI technologies such as MS Copilot, Claude, etc.
6. Experience in using tools to solve application performance issues.
7. Experience in metrics, analytics and logging.
8. Experience in working in an agile environment and working with cross-functional teams.
9. The proposed project person will be able to adhere to working on-site 5 days a week at CalSTRS Headquarters, West Sacramento, CA. (no points)

D. OFFER REQUIREMENTS AND INFORMATION

1. Time Schedule

CalSTRS will use its best efforts to adhere to the time schedule. However, CalSTRS reserves the right to amend the time schedule, as it deems necessary or appropriate.

Event	Date
Written Question Submittal Due Date	September 7, 2026 by 2:00 P.M., PT
Offer Due Date	September 16, 2026 by 2:00 P.M., PT
Estimated Start Work Date	November 2026

2. **Offer Requirements**

To be eligible, an Offer must include all of the following listed attachments and information:

- a. **Attachment I, Information and Offer Sheet**
- b. **Attachment II, Proposed Project Person Skill Summary Sheet**
- c. **Attachment III, Proposed Project Person Business Reference Sheet**
- d. **Proposed Project Person's Resume**
- e. **Current California Multiple Award Schedule (CMAS) Agreement**

One (1) copy of the Respondent's current, completed and signed Information Technology CMAS agreement and all supplements issued by the Department of General Services.

- f. **Current General Services Administration (GSA) Agreement**

One (1) copy of the Respondent's current GSA agreement and pricing pages applicable to the Respondent's Information Technology CMAS contract, which includes the personnel classifications, hourly rates, and minimum qualifications.

3. **Submission of Offer**

- a. All offers must be submitted to CalSTRS via email to ITProcurement@CalSTRS.com. If Respondents encounter any difficulties sending their offer, they must promptly notify CalSTRS Procurement.
- b. Offers must be received no later than the offer due date and time. Offers received after the specified date and time may be rejected.
- c. CalSTRS will only accept **ONE** offer submission per Respondent. Only ONE file attachment is allowed and must be in the form of .PDF (reduced file size) or a compressed zip file. The file title must not exceed thirty (30) characters and must include the Respondent Firm name and ten-digit RFO number (i.e. *Vendor A, 5000001234*). The file attachment must include all required documents as listed in section D.2. Offer Requirements of this RFO.
- d. It is the Respondent's responsibility to respond with all data/information requested; provide data/information that is deemed adequate for CalSTRS to determine/verify the proposed project person's ability to perform the tasks/activities defined in Attachment V, Statement of Work; and submit all data/information in the Offer format described in Section D, Subsection 2, Offer Requirements.
- e. It is the Respondent's responsibility to check for and review any addenda and consider such modifications when preparing its submissions.

- f. By submittal of an Offer, the Respondent declares that any proposed project person is in compliance with all experience, qualification, and education requirements stipulated in the Respondent's applicable Leveraged Procurement Agreement.
- g. If a Respondent has assigned contract person to CalSTRS under an existing agreement, the Respondent should not offer the same contract person for this RFO if the current term of the existing agreement and the estimated start of these RFO services will overlap. These Offers, if received, may be rejected at CalSTRS discretion.
- h. This RFO and all Offers in response to this RFO will be made a part of the resulting contract file. All documents submitted in response to this RFO will become the property of the State of California and may be subject to review by or release to the public under the California Public Records Act, Government Code section 7920.000 et seq.
- i. CalSTRS encourages Respondents to submit their Offers early.
- j. CalSTRS accepts no responsibility for any technical difficulties associated with the electronic submission and transmission of any Offer.
- k. CalSTRS will not disseminate the competitive processes and attachments hereto in any other format (i.e. Microsoft Word).
- l. Costs for developing Offers and in anticipation of award of an agreement are entirely the responsibilities of the Respondents and shall not be charged to CalSTRS.
- m. Respondents may modify their Offer, after its submission, by withdrawing their original Offer and resubmitting a new Offer prior to the Offer Due Date. Offer modifications submitted in any other manner, oral or written, or after the Offer Due Date will not be considered. Respondents may withdraw their own Offer by submitting a written withdrawal request to the CalSTRS Contact via email at ITProcurement@CalSTRS.com. Respondents may thereafter submit a new Offer prior to the Offer Due Date.
- n. CalSTRS may modify the RFO prior to the Offer Due Date by issuing an addendum.
- o. Respondents are cautioned to not rely on CalSTRS to discover and report to the Respondent any defects or errors in the submitted documents. Respondents, before submitting their documents, should carefully proofread for errors and ensure adherence to the RFO requirements.
- p. CalSTRS reserves the right to cancel this RFO at any time and has the right to reject all Offers. CalSTRS is not required to award an agreement.

4. Comparison Process

- a. Upon receipt, Offers will be checked for the presence or absence of required content. Incomplete Offers may be rejected. No assumptions will be made by CalSTRS regarding the intentions of the Respondent in submitting the Offer.

- b. Offers and any subsequent presentations should be submitted with the most favorable terms the Respondent can offer.
- c. If CalSTRS is unable to execute an agreement with the most qualified and responsible Respondent, CalSTRS reserves the right to award the agreement to the next qualified and responsible Respondent.
- d. Offers will be reviewed to determine best value using the following phases:

PHASES		
1	PREQUALIFICATION OF MINIMUM ADMINISTRATIVE AND TECHNICAL QUALIFICATIONS	Pass/Fail
2	TECHNICAL QUALIFICATION REVIEW	70 points
3	COST COMPARISON	30 points
PHASE 2 + PHASE 3 SCORE		100 points
4	INTERVIEWS	100 points
	REFERENCE CHECKS (OPTIONAL)	Pass/Fail
5	COST NEGOTIATIONS	Pass/Fail

- 1) In Phase 1, the Respondent's offer will be reviewed for compliance with the minimum qualifications, content and format requirements of the RFO. Both the minimum administrative and technical qualifications must be met as specified in Section C, Qualifications Requirements. Failure to satisfy any of part of prequalification may result in the immediate disqualification of the offer and/or applicable proposed project person.
- 2) Proposed project personnel who meet the minimum qualifications will move to Phase 2, Technical Qualification Review. Each proposed project person's expertise, experience, and education will be reviewed and scored based on the information provided in their Attachment II, Skill Summary Sheet (which also includes desirable qualifications), and resume.
- 3) In Phase 3, Cost Comparison, the hourly rate provided in the Respondent's Attachment I, will be scored using the cost formula indicated below. The Respondent's proposed project person with the lowest hourly rate will receive the full allotment of points. All other Respondents' proposed project personnel will be scored as follows:

$$\frac{\text{Lowest Hourly Rate} \times \text{Maximum Number of Points (30)}}{\text{Personnel's Proposed Hourly Rate}} = \text{Personnel's Score}$$

- 4) In Phase 4, highest scoring proposed project person(s) after Phase 2, Technical Qualification Review and Phase 3, Cost Comparison shall be invited for one or more rounds of interviews. Reference checks may be conducted.
- 5) In Phase 5, CalSTRS will negotiate rates with the Respondent whose proposed personnel is the highest ranking from Phase 4. If the initial highest ranking proposed project person is no longer available and/or does not pass Phase 5, Cost Negotiation, CalSTRS reserves the right to move to the next highest ranking proposed project person from Phase 4.

5. Award

- a. If CalSTRS enters into an agreement, it will be with the highest scoring responsible and responsive Respondent(s)/Proposed Personnel, as detailed above, subject to optional reference checks including passing the cost negotiation phase, and satisfying all the requirements for this RFO. Respondents should review the attached Sample Agreement for a sample of the agreement that will be awarded.
- b. If CalSTRS is unable to execute an agreement with the highest scoring Respondent(s)/Proposed Personnel, CalSTRS reserves the right to award to the next highest scoring responsive Respondent(s)/Proposed Personnel in line.
- c. Multiple project personnel may be selected from this RFO.
- d. The Respondent, if awarded an agreement, must register in the CalSTRS integrated financial system, the SAP Business Network. This portal provides direct access to administering product and service delivery with CalSTRS. Click on the hyperlink to register: <https://s1.ariba.com/Sourcing/Main/ad/selfRegistration?realm=calstrs>.
- e. If at any time during or at the conclusion of this RFO process CalSTRS determines that, in its opinion, the results of this process are unsatisfactory, CalSTRS reserves the right to cancel this RFO, discontinue this process and decline to award an agreement.
- f. In the event of a tie, (i.e. two Respondent's proposed project persons with the same highest score), the award shall be determined by a coin toss.

6. Payment Structure

The payment structure for activities performed under Attachment V, Statement of Work, is hourly.

Invoices shall be submitted in triplicate not more frequently than monthly in arrears.

Invoice(s) must include: 1) Purchase Order Number, 2) Contractor's name, address and telephone number, 3) total amount of invoice, 4) copies of the Contractor's weekly status reports that cover the invoice dates, and 5) a copy of the timesheet approved/signed by the CalSTRS Contract Manager that covers the invoice dates.

7. Services or Procurement Resulting from Agreement

No person, firm, or subsidiary thereof awarded an agreement resulting from this RFO may submit a bid for, nor be awarded a contract for, the provision of services, procurement of goods or supplies, or any other related action which is required, suggested, or otherwise deemed appropriate in the end product of an agreement resulting from this RFO. (Public Contract Code §10365.5).

8. Workers' Compensation/Employer's Liability Insurance

Contractor shall maintain statutory workers' compensation and employer's liability coverage for all its employees who will be engaged in the performance of the agreement, including special coverage extensions where applicable.

9. Security

Contractor shall perform a background investigation on all of Contractor's employees, subcontractors and agents assigned to perform the services, or any part of the services, pursuant to the agreement (the "Contractor Personnel"), per the provisions of the attached Sample Purchasing Authority Purchase Order Agreement, Section G - Affirmative Covenants, Item 10 – Security, and must demonstrate compliance with Exhibit E, CalSTRS Contractor Background Investigation Policy. CalSTRS reserves the right to conduct a background investigation on the Contractor's personnel, at its sole discretion.

ATTACHMENT I

Information and Offer Sheet

Respondent Firm Name

Firm Address

Street Address	
City, State, Zip Code	

Information Technology CMAS & Small Business / DVBE Certification

CMAS Number	
CMAS Term Dates	
Certified Small Business Enterprise (Yes or No) If Yes, provide DGS certification number	
Certified Disabled Veteran Business Enterprise (Yes or No) If Yes, provide DGS certification number	

Administrative Contact

Name and Title	
Office Telephone # (Include area code)	
Cell Telephone # (Include area code)	
Email Address	

Authorized Signer

Name and Title	
Office Telephone # (Include area code)	
Cell Telephone # (Include area code)	
Email Address	

Proposed Project Personnel and Rate

	Proposed Project Person #1 (mandatory)
Name of Proposed Project Person	
CMAS Job Title (Must be a job title listed in the <i>Available Products and/or Services</i> of your CMAS or TDDC MSA)	
CMAS (GSA) or TDDC MSA Hourly Rate	
Discount Hourly Rate Offered	

ATTACHMENT II

Proposed Project Person Skill Summary Sheet

This sheet must be completed by each Proposed Project Person.

Proposed Project Person Name

The proposed project person's expertise, experience, and education will be reviewed and scored based on the information including descriptions provided in this Attachment (which also includes desirable qualifications), and resume.

Follow the format prescribed below. The work experiences, skills and abilities listed in each description must be verifiable by proposed personnel references and resumes. A statement such as, *Refer to Resume*, is not acceptable. All fields must be completed.

MINIMUM TECHNICAL QUALIFICATIONS

1. A minimum of seven (7) years of experience in Software-as-a-Service (SaaS) application implementation, enhancement, and testing.	YES/ NO	TOTAL NO. OF YEARS	
Do you meet the above minimum qualification?			
Provide a detailed description of specific work experience that meets the minimum qualification.			
<u>Description</u>			
Employer and Work Location(s)	Date Range(s)		No. of Years
	From (MM/YYYY)	To (MM/YYYY)	

2. A minimum of seven (7) years of experience in technical and administrative support of SaaS applications, such as researching technical issues, debugging and resolving issues in a timely manner.		YES/ NO	TOTAL NO. OF YEARS	
Do you meet the above minimum qualification?				
Provide a detailed description of specific work experience that meets the minimum qualification.				
<u>Description</u>				
Employer and Work Location(s)		Date Range(s)		No. of Years
		From (MM/YYYY)	To (MM/YYYY)	

3. A minimum of seven (7) years of experience in cloud-based technologies such as AWS (e.g., Redis, Lamda, CloudWatch, etc.) and Azure.		YES/ NO	TOTAL NO. OF YEARS	
Do you meet the above minimum qualification?				
Provide a detailed description of specific work experience that meets the minimum qualification.				
<u>Description</u>				
Employer and Work Location(s)		Date Range(s)		No. of Years
		From (MM/YYYY)	To (MM/YYYY)	

4. A minimum of seven (7) years of experience in Software Development Life Cycle (SDLC) such as analyzing, solutioning, detail design, development, testing, automation and deployment.	YES/ NO	TOTAL NO. OF YEARS	
Do you meet the above minimum qualification?			
Provide a detailed description of specific work experience that meets the minimum qualification.			
<u>Description</u>			
Employer and Work Location(s)	Date Range(s)		No. of Years
	From (MM/YYYY)	To (MM/YYYY)	

For each **DESIRABLE QUALIFICATION**, give a brief description of specific work experience that meets/exceeds the criteria and demonstrates the number of **YEARS** entered, as applicable.

Follow the format prescribed below. The work experiences, skills and abilities listed in each description must be verifiable by proposed personnel references and resumes. A statement such as, *Refer to Resume*, is not acceptable.

DESIRABLE QUALIFICATIONS

1. A minimum of five (5) years of hands-on coding experience in algorithm and data structures.	NO. OF YEARS
<u>Description</u>	

2. Experience with technical integration between SaaS solutions and the ServiceNow “Now Platform” including but not limited to Incident Management, Change Management, Service Level Management, and Service Catalogue.	NO. OF YEARS
<u>Description</u>	
3. Experience in maintaining and administering ServiceNow Information Technology Service Management (ITSM), Information Technology Asset Management (ITAM), and Information Technology Operations Management (ITOM).	NO. OF YEARS
<u>Description</u>	
4. Extensive experience in using, defining, and generating reports (e.g., status, statistics, analysis) from ServiceNow for communication and periodic reporting of SaaS applications and solutions across the enterprise.	NO. OF YEARS
<u>Description</u>	
5. Experience with AI technologies such as MS Copilot, Claude, etc.	NO. OF YEARS
<u>Description</u>	
6. Experience in using tools to solve application performance issues.	NO. OF YEARS
<u>Description</u>	
7. Experience in metrics, analytics and logging.	NO. OF YEARS
<u>Description</u>	

8. Experience in working in an agile environment and working with cross-functional teams.	NO. OF YEARS
<u>Description</u>	
9. The proposed project person will be able to adhere to working on-site five (5) days per week at CalSTRS Headquarters, West Sacramento, CA. If no, provide a short explanation. (no points)	YES/ NO
<u>Description</u>	

ATTACHMENT III

Proposed Project Person Business Reference Sheet

One sheet must be completed for each Proposed Project Person.

Proposed Project Person Name

Business references should be able to verify the proposed project person's experiences, within the last 10 years, and to verify the other information provided regarding such person.

REFERENCE 1

Name of Company/Agency	
Company Address City, State	
Contact Person (Name and Title)	
Contact Telephone # (Include area code)	
Contact Email Address	
Dates of Service (Include years and months)	

REFERENCE 2

Name of Company/Agency	
Company Address City, State	
Contact Person (Name and Title)	
Contact Telephone # (Include area code)	
Contact Email Address	
Dates of Service (Include years and months)	

REFERENCE 3

Name of Company/Agency	
Company Address City, State	
Contact Person (Name and Title)	
Contact Telephone # (Include area code)	
Contact Email Address	
Dates of Service (Include years and months)	

ATTACHMENT IV

Frequently Asked Questions

The following are frequently asked questions as it pertains to this RFO. Respondents are responsible for reviewing these questions and responses. If this RFO accepts clarifications/questions, see instructions located on page 2 for how to submit written questions and the deadline to ensure a response.

Q.1. Is this a new position?

A.1. Yes.

Q.2. If there is an incumbent, are they eligible to be considered for this position?

A.2. N/A.

Q.3. Will phone/webcam interviews be an option if interviews are conducted?

A.3. Yes, CalSTRS may consider interviews using online collaboration platforms. CalSTRS will determine the appropriate platform to use. However, please select a resource that can attend interviews in person for the final round of interview(s).

Q.4. What is the anticipated award and start dates for the contract?

A.4. See RFO Section D.1., Time Schedule.

Q.5. Is there a “remote working” option?

A.5. See RFO Section A., Introduction.

Q.6. Is the RFO available in a Word document format?

A.6. In order to maintain the format prescribed, CalSTRS will not disseminate the RFO in Microsoft Word or any other format. It is the Respondent’s responsibility to develop and format a response, which may include the use of Microsoft Word, Adobe or other software and functions (i.e. prepare, convert, etc.), to provide all the required information and documents listed in the RFO.

Q.7. Is a CMAS required to respond to this RFO?

A.7. Yes.

Q.8. How do we become a CMAS vendor?

A.8. Business Entities interested in becoming a CMAS contractor may view the Department of General Services [site](#) for additional information.

Q.9. Which classification do I list on Attachment I if it does not match the CalSTRS position title?

A.9. Respondents may submit a classification that has similar skills/experience and that is an available service listed on their CMAS as long as all Minimum Qualifications of this RFO are met.

Q.10. What if a proposed project person I submitted is no longer available at time of contract award, can I submit a new proposed project person?

A.10. Award is based on each individual proposed project person's score. If any highest scoring proposed project person is no longer available at time of contract award, then CalSTRS reserves the right to award the next highest scoring Respondent/proposed project person in line.

Q.11. What is the estimated budget for this RFO?

A.11. In an effort to obtain competitive pricing, CalSTRS will not disclose this information.

Q.12. How to become a business partner with CalSTRS?

A.12. Business Entities may become a business partner with CalSTRS by registering in CalSTRS integration on-line financial system, the SAP Business Network. For more information about the portal and additional registration requirements please visit the link <https://s1.ariba.com/Sourcing/Main/ad/selfRegistration?realm=calstrs>.

Q.13. How do I update my business information (i.e. address, tax ID, entity name) with CalSTRS?

A.13. Business Entities will need to complete a Business Partner Form. To request the form please email Partners@CalSTRS.com.

Q.14. Does CalSTRS Headquarters have onsite parking for independent Contractors?

A.14. Monthly parking privileges are available for CalSTRS employees only. Independent contractors are responsible for seeking alternative parking locations. One option may be the Ziggurat parking garage at 601 Third Street, West Sacramento, CA. Other parking options can be found at [West Sacramento Parking Services](#).

ATTACHMENT V

Statement of Work

The Senior System Engineer (Contractor) shall have detailed knowledge and experience in Software-as-a-Service (SaaS) system implementation, enhancement, configuration, customization, validation, technical support, fixing defects, building dashboards and vendor and contract management. The Contractor shall maintain good working knowledge of SaaS applications such as ServiceNow, Salesforce, Electronic Content Management, Jama, and Riskconnect.

The Contractor must be able to perform all work on-site at the CalSTRS headquarters facility in West Sacramento, CA. At CalSTRS' discretion, a different approach (i.e., fully in-office, fully remote or different work hours) may be utilized based on CalSTRS business need and/or directive. Work must be performed during CalSTRS business hours and shall not be permitted on California State Holidays identified on the California Department of Human Resources website, unless pre-approved in writing by CalSTRS management. All work schedules must be pre-approved in writing by CalSTRS management and must adhere to all applicable CalSTRS policies and procedures. The Contractor is responsible for any travel costs (including travel time) that they may incur while providing the services identified in this Statement of Work.

Contractor shall perform the following, but not limited to:

1. Initiation and Evaluation Phase

Before the software is procured, the Contractor ensures it meets technical and organizational standards.

- **Technical Evaluation:** Review vendor architecture, Application Programming Interface (API) capabilities, and system compatibility.
- **Security & Compliance Auditing:** Verify System and Organization Controls 2 (SOC 2) and ISO 27001 compliance status.
- **Identity Readiness Planning:** Confirm the app supports Single Sign-On (SSO) with Entra ID.
- **Service Level Agreements (SLA) Verification:** Review vendor SLA for acceptable uptime and support response times.

2. Deployment and Integration Phase

During rollout, the Contractor builds the infrastructure required for users to access the tool.

- **Identity & Access Management (IAM):** Integrate the application with the identity provider (e.g., Entra ID).
- **Role-Based Access Control (RBAC):** Define permissions, user groups, and admin roles.
- **Network & Endpoint Security:** Configure IP whitelisting, Conditional Access policies, and Mobile Device Management (MDM) profiles.
- **Data Integration:** Connect APIs and data pipelines to existing internal systems or databases.

3. Operational Management Phase

The Contractor must manage the daily phase of maintaining availability, security, and user support.

- **User Lifecycle Management:** Oversee daily onboarding, offboarding, and transfer requests.
- **Monitoring & Alerting:** Track application uptime, API latency, and vendor status pages.
- **Incident Response:** Troubleshoot outages, manage vendor support tickets, and communicate downtime to users.

4. Optimization and Governance Phase

The Contractor must continually refine the footprint to control costs and maintain compliance.

- **Software as a Service (SaaS) Spend Optimization:** Audit usage metrics to reallocate or cancel inactive, expensive licenses.
- **Feature Lifecycle Management:** Test and roll out vendor updates, new features, and major user interface (UI) changes.
- **Regular Compliance Audits:** Conduct quarterly user access reviews to ensure permissions match current job roles.

5. Decommissioning and Offboarding Phase

When replacing or retiring a SaaS app, the Contractor securely removes it from the enterprise environment.

- **Data Extraction & Archival:** Download all enterprise data, audit logs, and configurations in reusable formats.
- **Termination of Access:** Disable SSO integrations, API keys, and System for Cross-domain Identity Management (SCIM) to prevent access leaks.
- **Data Destruction Verification:** Request a formal certificate of data erasure from the vendor.
- **Contract and Domain Name System (DNS) Cleanup:** Coordinate contract termination with procurement and delete related DNS records or subdomains.

Transfer of knowledge to appropriate CalSTRS employees is required, along with any requested materials and content for transfer of knowledge.

Completion Criteria

Deliverables/tasks will include all work assignments identified to be completed. Deliverables/tasks are considered complete after CalSTRS' quality assurance process is completed and approval is granted by designated CalSTRS' reviewers.

Performance and timeliness of all deliverables/tasks will be monitored by CalSTRS via the submission of Contractor's weekly status reports and through status meetings. Status and actual hours will be reported by Contractor on a weekly basis for the deliverables/tasks assigned. Each deliverable/task will be tracked via the appropriate program/project schedule and budget in order to monitor progress toward the completion of the deliverables/tasks and milestones.

**AGREEMENT NUMBER CW#####
BETWEEN CALIFORNIA STATE TEACHERS' RETIREMENT SYSTEM
AND <INSERT CONTRACTOR NAME>**

A. GENERAL RESPONSIBILITIES

Contractor

The California State Teachers' Retirement System, also known as CalSTRS, and <Insert Contractor Name>, also known as Contractor, agree to the following terms and conditions, in addition to those identified in the State of California, Multiple Award Schedule (CMAS) No. XXXX. See Exhibit A, Statement of Work (SOW).

B. AGREEMENT CONTACTS

1. Contractor

Contractor liaison for services shall be XXXX at telephone number (XXX) XXX-XXX and E-mail address [XXXX](#).

2. CalSTRS

- a) CalSTRS Business Contract Liaison for services shall be (Insert name) at E-mail address [XXX@CalSTRS.com](#) for questions related to the services.
- b) CalSTRS Business Contract Manager for services shall be (Insert name) at telephone number (916) 414-XXXX, and E-mail address [XXX@CalSTRS.com](#) for questions related to the services.

C. TERM

The term of this Agreement shall be from <Month, Date, Year> through <Month, Date, Year> with the option to extend up to <insert #> additional months if the Contractor's CMAS (identified above) is current prior to the term expiring.

D. FEES

The total amount of this Agreement shall not exceed \$XXX.XX, unless amended in writing, approved by all required authorities, and additional funds are authorized. Fees shall be calculated as follows:

<u>Hours</u>	<u>Position</u>	<u>Per Hour</u>	<u>Amount</u>
X,XXX	<Insert CalSTRS Working Title>	\$XXX.XX	\$XXX.XX
	<Insert GSA Classification>		

E. BUDGET DETAIL AND PAYMENT PROVISIONS

1. Invoicing and Payment

- a) For services satisfactorily rendered, and upon receipt and approval of the invoices, CalSTRS agrees to compensate the Contractor for actual expenditures incurred in accordance with the rates specified herein and made a part of this Agreement.
- b) Invoices shall be submitted not more frequently in monthly arrears through the following:
 - 1. The supplier submits their invoices through the SAP Business Network.
 - 2. If contractor/supplier has not registered, to do business with CalSTRS, on the SAP Business Network:
 - a. Supplier must contact Partners to create an SAP Business Network account to facilitate invoicing and payment.
 - b. Supplier will contact their Business Area Liaison for assistance in submitting an invoice.
- c) Invoice(s) must include: 1) Purchasing Authority Purchase Order Number, 2) Contractor's name, address and telephone number, 3) total amount of invoice, 4) copies of the Contractor's weekly status reports that cover the invoice dates, and 5) a copy of the timesheet approved/signed by a State Manager that covers the invoice dates.

2. Budget Contingency Clause

- a) It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, CalSTRS shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.
- b) If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, CalSTRS shall have the option to either cancel this Agreement with no liability occurring to CalSTRS or offer an agreement amendment to Contractor to reflect the reduced amount.
- c) Pursuant to the Teachers' Retirement Board (board) Governance Manual, any Agreement which exceeds \$1,000,000 in cumulative value must be approved by the board. If the Agreement term spans multiple fiscal years and board approval of the cumulative fiscal year value is required, it is mutually agreed that if the board does not approve funding for current year and/or any subsequent years, this Agreement shall be of no further force and effect.

3. Prompt Payment Clause

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with section 927.

F. GENERAL TERMS AND CONDITIONS

1. Approval

This Agreement is of no force or effect until signed by both parties. Contractor may not commence performance until approval has been obtained.

2. Titles/Section Headings

Titles or headings are not part of this Agreement, they are for convenience of reference only, and shall have no effect on the construction or legal effect of this Agreement.

3. Choice of Law

This Agreement and any controversy or claim arising out of or relating to this Agreement, or the breach thereof shall be administered, construed, governed and enforced according to the laws of the State of California (without regard to any conflict of laws provisions) to the extent such laws have not been preempted by applicable federal law. Any suit brought hereunder (including any action to compel arbitration or to enforce any award or judgment rendered thereby) shall be brought in the state or federal courts sitting in Sacramento, California, the parties hereby waiving any claim or defense that such forum is not convenient or proper. Each party agrees that any such court shall have in personam jurisdiction over it and consents to service of process in any manner authorized by California law.

4. Unenforceable Provision

In the event that any provision of this Agreement is unenforceable or held to be unenforceable, then the parties agree that all other provisions of this Agreement have full force and effect and shall not be affected thereby.

5. Amendment

No amendment or variation of the terms of this Agreement shall be valid unless made in writing and signed by the parties. No oral understanding or agreement not incorporated in the Agreement is binding on any of the parties.

6. Force Majeure

Neither party shall be liable to the other for delay in or failure of performance, nor shall any such delay in or failure of performance constitute default, if such delay or failure is caused by "Force Majeure." Such causes may include, but are not restricted to, Acts of

God or of the public enemy, acts of the State in its sovereign capacity, fires, floods, power failure, disabling strikes, epidemics, quarantine restrictions, and freight embargoes.

Contractor confirms that the goods/services to be provided to CalSTRS are not affected by the current COVID-19 Pandemic and that Contractor is able to perform under the Agreement.

7. Signatures & Counterparts

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. The parties agree to the terms of this Agreement and have caused this Agreement and its exhibits to be signed by their duly authorized representatives. Any manually executed signature page to this Agreement and its exhibits delivered by a party by facsimile or electronic mail in .PDF form shall be deemed to be an original signature hereto. Additionally, CalSTRS may provide the option for the parties to electronically sign this Agreement and exhibits via DocuSign or by other electronic means prescribed by CalSTRS. Any counterpart delivered using any of foregoing methods shall be deemed to have been duly and validly delivered with the same force and effect as original signatures, which together shall constitute one and the same instrument.

8. Intellectual Property

Contractor expressly acknowledges and agrees that all discoveries, inventions, processes, designs, plans, works of authorship, and trade secrets, whether of a technical nature or not, made or developed by Contractor alone or in conjunction with any other person or entity while accomplishing the Agreement (Intellectual Property), shall be the sole and exclusive property of CalSTRS and CalSTRS may use or reuse the Intellectual Property, in whole or in part, in all media, whether now or later existing, throughout the universe in perpetuity, including but not limited to the exclusive right to reproduce, perform and exploit the Intellectual Property, and all information regarding the Intellectual Property, concurrent with the discovery or development of the Intellectual Property. If the Intellectual Property or the results and proceeds thereof constitute "works of authorship" within the scope of U.S. Copyright Law, the foregoing shall be deemed "works made for hire" and CalSTRS shall be considered the sole author and owner of all rights comprised in the copyright and/or patent thereof and shall have the exclusive right to seek patent and/or copyright protection in CalSTRS name. In the event that any Intellectual Property does not constitute "works made for hire," Contractor hereby assigns all rights thereto exclusively to CalSTRS for any and all purposes of CalSTRS. At all times during its term and after the termination of the Agreement, Contractor shall assist CalSTRS in obtaining and maintaining, for CalSTRS benefit, protection of the Intellectual Property and Contractor shall execute and cause its subcontractors to execute such further instruments as CalSTRS may reasonably require as evidence of ownership of such rights. Contractor agrees that he/she will not use or disclose any Intellectual Property owned by CalSTRS without the express written permission of CalSTRS.

G. AFFIRMATIVE COVENANTS

1. Reports and/or Meetings

- a) Contractor shall provide oral or written progress reports as requested by CalSTRS to determine if Contractor is performing to expectations or is on schedule, to provide communication of interim findings, and shall afford occasions for discussing and resolving problems encountered.
- b) Contractor shall meet with CalSTRS staff and/or the board upon request to discuss progress on the Agreement or to present findings, conclusions and recommendations.

2. Additional Documents

Contractor and CalSTRS agree to execute such additional documents, and perform such further acts, as may be reasonable and necessary to carry out the provisions of this Agreement.

3. Reportable Interests

Contractor shall not directly or indirectly receive any benefit from recommendations made to CalSTRS and shall disclose to CalSTRS any personal investment or economic interest of Contractor which may be enhanced by the recommendations made to CalSTRS. Contractor acknowledges that CalSTRS is subject to provisions of the Fair Political Practices laws of California (Government Code section 81000, et seq., and all regulations adopted thereunder, including, but not limited to, Title 2, California Code of Regulations, section 18700) and Contractor shall comply promptly with any requirement thereunder. If required by law, Contractor shall require its Key Personnel named, and all later substitutions therefore, to file Statements of Economic Interest (Title 5, California Code of Regulations, section 22000 et seq.). All such reports shall be filed simultaneously with CalSTRS.

4. Key Personnel

Exhibit B, Contractor Name's Key Personnel, names certain members of Contractor's staff (key individuals) who will perform the conduct described in the scope of services and exercise a significant decision making role in the delivery of services under this Agreement. These personnel shall be hereafter referred to (both individually and collectively) as "Key Personnel."

- a) Contractor shall not substitute, replace or reassign Key Personnel without CalSTRS prior approval. However, with CalSTRS prior approval, the parties may agree in writing to a change in these Key Personnel. The writing shall become a part of this Agreement.

- b) This Agreement may be terminated immediately, in CalSTRS sole discretion and upon written notice from CalSTRS to Contractor, because of any change in or departure of Contractor's Key Personnel.

5. Changes in Control, Organization or Key Personnel

Contractor shall promptly, and in any case within five (5) calendar days, notify CalSTRS in writing: 1) if any of Contractor's representations and warranties, as set forth in this Agreement, cease to be true at any time during the term of this Agreement; 2) of any change in Contractor's staff who exercise a significant administrative, policy, or consulting role under this Agreement, including without limitation the Key Personnel; 3) of any change in the majority ownership, control, or business structure of Contractor; or 4) of any other material change in Contractor's business, partnership or corporate organization. All written notices from Contractor under this provision shall contain sufficient information to permit CalSTRS to evaluate the changes within Contractor's personnel or organization under the same criteria as was used by CalSTRS in its award of this Agreement to Contractor. Contractor agrees to provide CalSTRS with such additional information as CalSTRS may request.

6. Contractor Employee Relationship for CMAS Vendors

Contractor understands and acknowledges that the personnel provided to CalSTRS under this Agreement are the employees of the Contractor or Independent Contractors who have a contractual relationship with the Contractor. Contractor agrees to indemnify, defend and hold CalSTRS harmless from any and all claims made against it including, but not limited to, claims for salaries, liability for tax withholding, workers' compensation, disability or miscellaneous employment benefits, whether based on tort, contract or other theories of recovery arising out of injury, disability, or death of Contractors' employees or Independent Contractors.

7. Warranty of Compliance – Termination

Contractor warrants that it has implemented and will enforce CalSTRS Contractor Background Investigation Policy, Exhibit E, and agrees that it will promptly notify CalSTRS of any changes which become known to them which would affect their compliance with said guidelines. In the absence of any notice of such information subsequent to the hiring of the Contractor Employee by Contractor, CalSTRS will rely on the on-going compliance statement made by Contractor. In the event CalSTRS finds that Contractor has failed to properly perform the background check or fails to provide CalSTRS with information subsequently known to Contractor after such investigation, CalSTRS has the right to immediately terminate the Agreement with Contractor.

8. Knowledge Transfer

Where appropriate, Contractor's obligations under the terms of this Agreement include a "knowledge transfer" to CalSTRS. "Knowledge transfer" is defined as personal and/or technical knowledge or information which will enable, or enhance the ability of, CalSTRS staff to maintain and operate contracted-for programs, equipment and facilities.

If the Agreement includes the purchase of equipment, “knowledge transfer” shall also include education and training, including all relevant documentation, to enable CalSTRS to maintain the equipment based on Contractor’s methodology. The Contractor agrees that CalSTRS may reproduce such documentation for its own use in maintaining the equipment.

Any additional training or instruction necessary to realize the “knowledge transfer” shall be provided at no additional cost to CalSTRS.

9. Information Security and Privacy

Contractor, in the course of its duties, may handle investment, financial, accounting, statistical, personal, technical and other data and information relating to CalSTRS and its members. All such information is confidential, and, unless permitted by CalSTRS in writing, Contractor shall not disclose such information, directly or indirectly, or use it in any way, either during the term of the Agreement or any time thereafter, except as required to perform its duties under this Agreement. Any disclosure of information contrary to this provision shall be considered a material breach of this Agreement. Contractor warrants that only those who are authorized and required to use such materials will have access to them. Failure to comply with this provision will subject Contractor to liability, including all damages to CalSTRS and third parties.

Contractor shall comply with all information security and privacy obligations set forth in the CalSTRS Information Security and Privacy Addendum (Exhibit H), which is incorporated by reference into this Agreement. This addendum establishes the necessary security and privacy measures Contractor must implement, including but not limited to confidentiality obligations, security controls, incident response, indemnification, and data handling requirements.

As part of these obligations:

- a) Exhibit I – Confidentiality, Non-Disclosure and Acceptable Use Agreement (ISO 1948): Contractor’s Authorized Representative, with authority to act on behalf of the entity, must sign Exhibit I prior to engaging in work with CalSTRS.
- b) Exhibit J – CalSTRS Minimum Information Security Requirements (MISR): Contractor shall adhere to the security requirements detailed in Exhibit J as part of its overall information security obligations.

Failure to comply with Exhibits I and J may be deemed a material breach of the contract, at CalSTRS discretion.

10. Security

Contractor shall perform a background investigation on all of Contractor’s employees assigned to perform any part of the services hereunder, or who shall access any of CalSTRS Confidential Information (the “**Contractor Personnel**”). Contractor’s background investigation shall consist of the components prescribed in CalSTRS’

Contractor Background Investigation Policy (Exhibit E). All Contractor Personnel must successfully complete and pass Contractor's background investigation prior to providing services or accessing Confidential Information hereunder. Compliance with CalSTRS Contractor Background Investigation Policy must be affirmed with submission of a completed *Certification of Contractor's Employee Background Investigation Form* (Exhibit F) listing each of Contractor's Personnel. Contractor shall keep such form updated to reflect any changes to its Contractor Personnel. Contractor shall ensure that employees of its subcontractors or agents also satisfy appropriate background investigation criteria. Contractor shall provide CalSTRS (or its designee) with documentation providing evidence of Contractor's background investigation of Contractor Personnel upon the reasonable request of CalSTRS.

Further, all Contractor Personnel must submit to CalSTRS the Personal History Statement (Exhibit G) identifying any relatives of the contract employee that are CalSTRS members, beneficiaries, or employees.

11. Compliance with Statute, Regulations and Policies

Contractor warrants and certifies that in the performance of this Agreement, it will comply with all applicable statutes, rules, regulations, and orders of the United States and the State of California and agrees to indemnify CalSTRS against any loss, cost, damage or liability by reason of Contractor's violation of this provision.

H. CONTRACT CERTIFICATION CLAUSES

1. Contractor Name Change

An amendment is required to change the Contractor's name as listed on this Agreement. Upon receipt of legal documentation of the name change CalSTRS will process the amendment. Payment of invoices presented with a new name cannot be paid prior to approval of said amendment.

2. Statement of Compliance – Nondiscrimination

Contractor's signature affixed hereon and dated shall constitute a certification under the penalty of perjury under the laws of the State of California that Contractor has, unless exempted, complied with the nondiscrimination program requirements of Government Code section 12990 (a)-(f) and Title 2, California Code of Regulations, section 11102 et seq.

3. Labor Code/Workers' Compensation

Contractor needs to be aware of the provisions which require every employer to be insured against liability for Worker's Compensation or to undertake self-insurance in accordance with the provisions within the Labor Code section 3700, and Contractor affirms to comply with such provisions, before commencing the performance of work in this Agreement.

4. Drug-Free Workplace Act of 1990 (Act)

Contractor will comply with the requirements of the Act and will provide a drug-free workplace by taking the following actions:

- a) Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations.
- b) Establish a Drug-Free Awareness Program to inform employees about:
 - 1. The dangers of drug abuse in the workplace;
 - 2. The person's or organization's policy of maintaining a drug-free workplace;
 - 3. Any available counseling, rehabilitation and employee assistance programs; and,
 - 4. Penalties that may be imposed upon employees for drug abuse violations.
- c) Every employee who works on the proposed Agreement will:
 - 1. Receive a copy of the company's drug-free policy statement; and,
 - 2. Agree to abide by the terms of the company's statements as a condition of employment on the Agreement.

Failure to comply with these requirements may result in suspension of payments under the Agreement or termination of the Agreement or both and Contractor may be ineligible for award of any future State agreements if CalSTRS determines that any of the following has occurred: (1) the Contractor has made false certification, or (2) violated the certification by failing to carry out the requirements as noted above. (Government Code section 8350 et seq.)

6. Unauthorized Alien

Contractor will comply with 8 USC §1324a et seq. and shall not knowingly employ or contract with an unauthorized alien to perform work.

7. Child Support Compliance Act

- a) The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable state and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with section 5200) of Part 5 of Division 9 of the Family Code; and
- b) The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.

I. SPECIAL TERMS AND CONDITIONS

1. Evaluation of Contractor

Pursuant to Public Contract Code section 10369, CalSTRS shall evaluate Contractor's performance under the terms and conditions of this Agreement within sixty (60) days after the completion of Contractor's performance under this Agreement. If the evaluation indicates unsatisfactory performance, a STD 4 (Contract/Contractor Evaluation) will be completed and a copy sent to the Department of General Services, Office of Legal Services, and to Contractor who may file a response to the evaluation. The evaluation and response shall remain on file for thirty-six (36) months and shall not be public records.

2. Third Party Economic Interest Disclosure Policy

a) Policy

The Third Party Economic Interest Disclosure Policy set forth in the Teachers' Retirement Board Governance Manual requires entities and Key Personnel engaging in business with CalSTRS to disclose campaign contributions, as defined under the California Political Reform Act, valued in excess of \$250, prohibits providing charitable contributions valued in excess of \$250, and gifts in excess of the current monetary limit established by the Fair Political Practices Commission, as well as requiring the periodic disclosure of campaign contributions, charitable contributions, and gifts. A copy of the current policy is attached as Exhibit C and Contractor is required to comply with its provisions.

b) Submission of Disclosures

Contractor (Entity) and each of its Key Personnel shall, with the signing of this Agreement and annually thereafter, submit disclosures of contributions and gifts described in this section on a form prescribed by CalSTRS. The current disclosure form required to be submitted is Exhibit D, Form 600-H Third Party Economic Disclosure. Exhibit D must be submitted on behalf of the Contractor (Entity) and each of its Key Personnel (those who signed Exhibit B). No other version of this form will be accepted (e.g., annual submittal or generic form downloaded from CalSTRS.com).

Annual disclosures shall be due by April 1st of each year and forms will be provided to Contractor and its personnel by CalSTRS.

c) Violation of Policy by Contractor

Any violation may lead to one or more of the following: (1) immediate termination of any agreement/contract, (2) CalSTRS withholding future payments on any existing agreement/contract, and/or (3) disqualification from future business with CalSTRS for a period of two years following a determination that a violation has occurred. These sanctions will be at CalSTRS' sole discretion and upon written

notice from CalSTRS to the entity. The general counsel shall provide a report of violations to the Audits and Risk Management (ARM) Committee.

d) Changes in Laws or Policy

CalSTRS reserves the right to amend, upon prior written notice, the above provisions to conform with any subsequent amendments to the political reform laws and CalSTRS policies.

J. TERMINATION

1. Termination at Option of CalSTRS

This Agreement may be terminated in whole or in part at any time upon thirty (30) calendar days' written notice by CalSTRS, for any reason. Upon receipt of a termination notice, Contractor shall promptly discontinue all services affected unless the notice specifies otherwise.

In the event CalSTRS terminates all or a portion of this Agreement for any reason, it is understood that CalSTRS will provide payment to Contractor for satisfactory services rendered prior to the termination, but not in excess of the maximum Agreement amount.

2. Termination for Default

CalSTRS may, by giving two (2) calendar days' written notice to Contractor, and without prejudice to any of its remedies, terminate this Agreement because:

- a) The Contractor failed to fulfill its obligations under this Agreement (including, but not limited to any attachments to this Agreement); or
- b) The Contractor provides inaccurate information or fails to provide information that the Contractor knew or should have known existed.

In the event of termination for default, CalSTRS shall pay Contractor only the reasonable value of the services rendered. At CalSTRS sole discretion, CalSTRS may offer an opportunity to cure any breach(es) prior to terminating for default.

3. Termination for Insolvency

Contractor shall notify CalSTRS immediately in writing in the event that Contractor files any federal bankruptcy action or state receivership action, any federal bankruptcy or state receivership action is commenced against Contractor, Contractor is adjudged bankrupt, or a receiver is appointed and qualifies. In the event of any of the foregoing events, or if CalSTRS determines, based on reliable information, that there is a substantial probability that Contractor will be financially unable to continue performance under this Agreement, CalSTRS may terminate this Agreement and all further rights and obligations immediately, by giving five (5) days' notice in writing in the manner specified herein.

4. Convenience

If after notice of termination for failure to fulfill agreement obligations, it is determined that Contractor had not so failed, the termination shall be deemed effective for the convenience of CalSTRS.

5. Completion

In the event of termination for default, CalSTRS reserves the right to take over and complete the work by agreement or other means. In such case, Contractor will be liable to CalSTRS for any additional cost incurred by CalSTRS to complete the work whether reimbursed or not.

6. Effect of Termination

All duties and obligations of CalSTRS and Contractor shall cease upon termination of this Agreement, except that:

- a) Each party shall remain liable for any rights, obligations, or liabilities arising from activities carried on by it under this Agreement prior to the effective date of termination.
- b) Contractor shall provide for the return of all records of CalSTRS to CalSTRS or its designee and shall cooperate fully to affect an orderly transfer of services.

<Insert Authorized Signer Name>

<Insert Contractor Firm Name>

Date

Select Signatory
California State Teachers' Retirement System

Date

Statement of Work

[To be inserted at time of contract award.]

SAMPLE

<Contractor Firm Name>
KEY PERSONNEL

Please list the names and titles of the personnel authorized to conduct business (deliver services) on behalf of the Contractor in a decision-making capacity:

Signature _____

Name _____

Title _____

Date _____

E-mail _____

Signature _____

Name _____

Title _____

Date _____

E-mail _____

Signature _____

Name _____

Title _____

Date _____

E-mail _____

Signature _____

Name _____

Title _____

Date _____

E-mail _____

TEACHERS' RETIREMENT BOARD GOVERNANCE MANUAL

G. Third Party Economic Interest Disclosure Policy

It is the policy of CalSTRS to conduct business with vendors, business entities and investment service providers, managers, partners and/or consultants in a manner which avoids potential or actual financial conflicts of interest. Consistent with this policy, certain disclosures involving campaign contributions, charitable contributions and gifts are required as set forth below.

1. Definitions

For purposes of this Third Party Economic Disclosure Policy only, the following definitions apply:

- a. Entity: The terms “Entity” and “Entities” mean any vendor, business entity or investment service provider, manager, partner or consultant doing business directly with CalSTRS.
- b. Key Personnel: The term “Key Personnel” means any individual associated with an Entity that:
 - i. Negotiates a contract between an Entity and CalSTRS; or
 - ii. Is a high-level officer or employee of an Entity who exercises primary responsibility for the work performed pursuant to a contract between an Entity and CalSTRS; or
 - iii. Directs or supervises Entity staff regarding work performed pursuant to a contract between an Entity and CalSTRS; or
 - iv. Provides services to CalSTRS as a “consultant” pursuant to Government Code sections 82019, 82048 and California Code of Regulations, Title 2, Section 18700.3.
- c. Gift: The terms “Gift and “Gifts” mean anything of value, whether tangible or intangible, real or personal property, goods or services, that provides a personal benefit to an individual when the individual does not provide full consideration for the value of the benefit received.

2. Campaign Contributions

All Entities and Key Personnel shall disclose campaign contributions, as defined under the California Political Reform Act, valued in excess of \$250, made to or on behalf of any existing CalSTRS board member, candidates for board member, controller, treasurer, superintendent of public instruction, CalSTRS officer or employee.

3. Charitable Contributions

All Entities and Key Personnel shall disclose any charitable contributions to a charitable entity, valued in excess of \$250 individually or in the aggregate in any calendar year, made at the request of any board member, or CalSTRS officer or employee.

4. Gifts

- a. No Entity or Key Personnel shall provide gifts to board members exceeding the current monetary limit established by the Fair Political Practices Commission individually or in the aggregate in any calendar year. The dollar amount of this limit is adjusted biennially in each odd numbered year to reflect the cost of living adjustments made by the Fair Political Practices Commission to the gift limit contained in Government Code section 89503.
- b. All Entities and Key Personnel shall disclose gifts aggregating more than \$50 in value made to board members, or to CalSTRS officers or employees.

5. Recusal

- a. Any board member who receives campaign contributions, charitable contributions, or gifts that individually or in the aggregate exceed the amount of \$250 in a calendar year from an Entity or Key Personnel shall recuse themselves from any involvement in a matter involving the maker of the contributions or gifts for a period of 12 months following the date of the most recent contribution or gift.
- b. Any board member who returns, donates, or reimburses the donor for gifts subject to these restrictions within 30 calendar days of receipt of the gift shall not be subject to the recusal requirement. Gifts may be returned, donated or reimbursed as specified in California Code of Regulations, Title 2, Section 18933.

6. Disclosure Filing Timeline

The disclosure of campaign contributions, charitable contributions, and gifts shall be made on the Third-Party Economic Interest Disclosure (Form 600-H) as follows:

- a. Upon submission of an initial application or proposal to do business with CalSTRS (for the preceding 12-month period).
- b. At the time a contract is entered into between the Entity and CalSTRS (to cover the interim period following the submission of a Form 600-H pursuant to subsection 6(A) above).
- c. Annually, on or before April 1 for the previous calendar year. You are not required to file an annual Form 600-H under this subsection

if a Form 600- H has been filed with CalSTRS in accordance with subsection (6)(B) between October 1 and December 31 of the preceding year.

- d. Within five (5) calendar days of a change in Key Personnel, the new Key Personnel shall file a Form 600-H.

7. Sanctions for Violation of Policy

The general counsel is responsible for causing an investigation of any reported violation of this policy. Any violation may lead to one or more of the following:

(1) immediate termination of any agreement/contract, (2) CalSTRS withholding future payments on any existing agreement/contract, and/or (3) disqualification from future business with CalSTRS for a period of two years following a determination that a violation has occurred. These sanctions will be at CalSTRS' sole discretion and upon written notice from CalSTRS to the entity. The general counsel shall provide a report of violations to the Audits and Risk Management (ARM) Committee.

8. Application of Policy

Nothing in this policy supersedes any provision of state law. Those Entities engaged in business with CalSTRS may also have reporting requirements under the Political Reform Act, California Government Code section 81000 et seq. Also, board members who are either elected to the board by a CalSTRS constituency or who are appointed to the board but also serve as an elected official of a local body are subject to Government Code section 84308, which prohibits the receipt, solicitation or direction of a campaign contribution of more than \$250 while a matter affecting a financial interest of the maker of the contribution is pending, and for three months following the date a decision is rendered on the matter. Section 84308 also requires recusal of the board member from any involvement in the matter if a contribution over \$250 has been received within the preceding 12 months, unless the contribution was returned no later than 30 days from the time the board member knew or should have known about the contribution and the matter involving the maker of the contribution.

Reference: Ed. Code, § 22363; Gov. Code, §§ 82019, 82048; Cal. Code Regs., tit. 2, § 18700.3. History: Amended December 7, 2006; Amended June 6, 2007; Amended February 7, 2008; Amended April 8, 2016; Amended January 31, 2019; Amended January 31, 2020 [to reflect gender-neutral language and change the California Code of Regulations citations in subsection 5(b) from section 18943 to section 18933]; Amended November 5, 2021 [updated Sanctions for Violation of Policy section.

Form 600-H

THIRD PARTY ECONOMIC INTEREST DISCLOSURE

Pursuant to Section 4, subsection G, of the Teachers' Retirement Board Governance Manual, entitled "Third Party Economic Interest Disclosure Policy", any Entity/Entities and its Key Personnel who engage in business with CalSTRS are required to make specific public disclosures.¹ Entities and each of their Key Personnel must complete and file separate forms. The below identified Entity/Entities or its Key Personnel hereby make the following disclosures. (Please attach other sheets if more space is needed for disclosure and indicate enclosures.)

Identification of Filer (Key Personnel or Entity – separate filings required)

Name of Entity:		Reported on behalf of Entity <input style="width: 20px; height: 20px;" type="checkbox"/>
Key Personnel or Person Making Disclosure:		

Relationship Category (Please choose the one that is most appropriate to this relationship): ☐ Investment If Other: ☐ Non-Investment Contractor / Consultant - Description of Service Provided:	Investment Asset Class If Other:
--	---

Mailing Address:					
	Number	Street	City/Locality	State/Province	Zip
Telephone:			E-mail Address:		

Filing and Disclosure Period

This disclosure of campaign contributions, charitable contributions, and gifts is in response to the following filing requirement:

☐	A. At Solicitation of an initial application or proposal to do business with CalSTRS (covers preceding 12-month period)
☐	B. At Contract/Agreement for execution of services (signature) to cover the interim period since the initial application
☐	C. Annual disclosure for the previous calendar year
☐	D. New Key Personnel

¹ See Teachers' Retirement Board Governance Manual Section 4, subsection G (1)(a) and (b) for definitions of Entity, Entities and Key Personnel.

Form 600-H

1. Disclosure of Campaign Contributions

Disclosure of Campaign Contributions valued in excess of \$250 made to or on behalf of any a) existing Teacher's Retirement Board member, b) candidates for Board member, Controller, Treasurer, and Superintendent of Public Instruction, and c) CalSTRS officer or employee. The term "contribution" is defined in the Political Reform Act regulations, in Title 2, California Code of Regulations (CCR) section 18215. If the business is an Investment Relationship, disclosure of campaign contributions made to the Governor or candidates for the governorship must also be made, according to CalSTRS' Campaign Contribution regulations in Title 5, CCR section 24010.

☐ **Nothing to report**

☐ Attachment is enclosed

Value of Contribution	Description if other than monetary	Date of Contribution	Identity of Recipient of Contribution

2. Disclosure of Charitable Contributions

Disclosure of charitable contributions valued in excess of \$250 made at the request of any Teachers' Retirement Board member or CalSTRS officer or employee to any charitable organization.

☐ **Nothing to report**

☐ Attachment is enclosed

Value of Contribution	Description of Contribution (monetary or in-kind)	Date of Contribution	Identity of Recipient of Contribution	Identity of Requester of Contribution

3. Disclosure of Gifts²

Disclosure of gifts, including meals, entertainment, or travel, valued in excess of \$50 made to any Teachers' Retirement Board member or CalSTRS officer or employee.

☐ **Nothing to report**

☐ Attachment is enclosed

Value of Gift	Description of Gift	Date Gift Given	Identity of Recipient of Gift

I have exercised all reasonable due diligence in preparing this disclosure statement on my own behalf or on behalf of the reporting entity identified above. I have reviewed this statement and to the best of my knowledge the information contained herein and in any attachments is true and complete. I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Signature

Title

Printed Name

Date

² See Teachers' Retirement Board Governance Manual Section 4, subsection G (1)(c), for definition of "Gift".

CONTRACTOR BACKGROUND INVESTIGATION POLICY

PURPOSE: It is the policy of the California State Teachers' Retirement System (CalSTRS) to require all Contractors who contract with CalSTRS to perform services to gather and consider relevant background history information in determining if certain of Contractor's employees ("Contractor Personnel") who provide services to CalSTRS meet the general standards for working with CalSTRS and safeguarding CalSTRS information.

POLICY: Contractor shall comply with all applicable law, rules and regulations related to conducting employee background investigations, including without limitation, the Fair Credit Reporting Act, the California Investigative Consumer Reporting Agencies Act and California Government Code §12952. Contractor shall be solely responsible for any failure to conduct its background investigations in compliance with applicable law.

In evaluating the suitability of a particular individual's work assignment with CalSTRS, Contractor must give particular emphasis to the business needs arising from CalSTRS' fiduciary responsibility for CalSTRS funds, its obligation to protect the personal data it holds and maintain the integrity of the retirement system, and its policy to provide a safe and secure workplace.

This includes, but is not limited to preventing contractors or Contractor Personnel from using their access to CalSTRS facilities, systems or data to:

- Carry out identity theft or related activities.
- Inappropriately alter member retirement benefits.
- Embezzle funds from CalSTRS.
- Engage in any activity that would damage CalSTRS' reputation or member trust.
- Initiate any act of workplace violence, discrimination, or sexual harassment.

Prior to allowing Contractor Personnel to perform work on behalf of CalSTRS under the Agreement or obtain access to CalSTRS information (a "CalSTRS Assignment"), Contractor is responsible for conducting an appropriate background investigation, including a criminal record check, credit check, civil check, reference check, and verification of education and previous employment as allowed by then applicable law (a "Background Investigation"), of any such Contractor Personnel. In addition, Contractor must review the driving records of any Contractor Personnel who may drive on CalSTRS-related business as a regularly assigned duty. The information gathered in this process is subject to strict confidentiality provisions in order to protect the privacy of those persons whose backgrounds are reviewed under this policy.

Contractor will review and evaluate all information obtained as part of its Background Investigation of any Contractor Personnel and will not assign any Contractor Personnel to a CalSTRS Assignment if the Contractor determines, based in whole or part on the information obtained as part of the Background

Investigation, that the Contractor Personnel is not suitable for the assignment. Examples of reasons for which Contractor Personnel may be unsuitable for CalSTRS assignment include:

Criminal Record Checks

1. Any conviction for any of the following offenses:
 - Any form of fraud, deceit or misrepresentation
 - Embezzlement
 - Forgery
 - Identity theft/stolen credit card use
 - Any other offense involving misappropriation of assets or resources, abuse of access to financial or personal records, unauthorized access to financial or personal records, falsification of documents or records, crimes of moral turpitude, or crimes which may be relevant to CalSTRS Assignment
2. Any conviction for offenses related to stealing such as the following:
 - Theft, burglary, carjacking or home invasion crimes
 - Shoplifting
 - Receiving stolen property
 - Bad checks
3. Any conviction for any violent crime for such an offense.

Contractor Personnel with convictions other than those specified above, may be deemed unsuitable for a CalSTRS Assignment when the record of convictions indicates or suggests to the Contractor a continuing pattern of behavior that is inconsistent with CalSTRS business objectives specified in the Background section, above.

Contractor is responsible for reviewing the civil litigation history of any Contractor to the extent permissible by applicable law. Contractor should not assign any Contractor Personnel to a CalSTRS Assignment if the individual's civil litigation history reveals that he or she lacks one or more of the general qualifications for a CalSTRS Assignment such as honest, integrity, and/or good judgement.

Credit Checks

Contractor is responsible for reviewing the credit history of any Contractor, consistent with applicable law. Contractor should not assign any Contractor Personnel to a CalSTRS Assignment if the individual's credit history reveals a continuing pattern of credit abuse that supports the conclusion that he or she lacks one or more of the general qualifications for a CalSTRS Assignment, such as honesty, integrity, and/or good judgment.

These determinations require careful case-by-case review of any credit problems, with particular emphasis on the following questions:

- Are the credit problems isolated to a particular point in time, or to a particular vendor with whom the individual may be having a dispute, or do they constitute a general pattern?
- Are there specific mitigating factors that explain the credit problems, such as illness or divorce?
- What effort has the individual made to correct the credit problems?
- How recent are the problems, and what has the credit record been since they occurred?

Reference Checks

Contractor should not assign any Contractor Personnel to a CalSTRS Assignment if a reference check gives Contractor reason to believe that the individual lacks one or more of the general qualifications for employment such as honesty, integrity, and/or good judgment.

Fraud in Securing Appointment

Any information Contractor Personnel provides for employment with or to provide services to Contractor (on applications, resumes, background questionnaires, etc.) must be substantively truthful. Should the Contractor determine that the information it did receive from any Contractor Personnel was not substantively truthful, it shall promptly remove such individual from the CalSTRS Assignment to the extent permissible under applicable law.

Driving Record Checks

A serious driving violation, such as driving under the influence of alcohol or drugs, or reckless driving, within the past three years, may disqualify Contractor Personnel from a CalSTRS Assignment, if the nature of the work performed for CalSTRS requires driving as a regularly assigned duty. Contractor must review driving records when driving a motor vehicle on a CalSTRS Assignment is a regularly assigned duty.

Prior to any Contractor Personnel performing services under the Agreement, Contractor shall certify that it has performed a Background Investigation of such Contractor Personnel, reviewed and verified the background information in a manner consistent with CalSTRS' Contractor Background Investigation Policy, and determined that the individual(s) is/are qualified for the CalSTRS Assignment. Such certification will be made with submission of the "Certification of Contractor's Employee Background Investigation" form, provided to Contractor by CalSTRS.

In addition, Contractor shall provide CalSTRS with each Contractor Personnel's completed Personal History Statement. Information the Contractor Personnel provides concerning relatives who are CalSTRS members or beneficiaries

and/or CalSTRS employees will be used to implement safeguards to prevent the individual from working on or accessing the records/accounts of his or her relatives.

Contractor shall review and investigate any relevant information it received or becomes aware of subsequent to the date of the Background Investigation regarding any Contractor Personnel. Contractor shall immediately notify the Human Resources Division of CalSTRS if it receives information which might lead the Contractor to believe any Contractor Personnel would be ineligible to work on a CalSTRS Assignment, as described in this CalSTRS Contractor Background Investigation Policy, had the Contractor known the information at the time it conducted the Background Investigation. Contractor shall promptly replace any such Contractor Personnel upon CalSTRS request. When requested by CalSTRS (generally annually), Contractor shall certify, on a form provided by CalSTRS, that it knows of no information that would affect the suitability of any Contractor Personnel to work on a CalSTRS Assignment.

Contractor shall retain documents and files received in the Background Investigation throughout the term of the Agreement, shall provide reasonable safeguards to ensure security and confidentiality of these documents and files, and will work cooperatively with CalSTRS to provide related data or information upon CalSTRS's reasonable request, consistent with applicable law.

Any request for a waiver of the policy provisions should be directed to the Director of the Procurement Management Division, who will thereafter forward the request to the CalSTRS CEO for consideration and approval, on a case-by-case basis. Exceptions to the Contractor Background Investigation Policy may include but are not limited to the following circumstances:

- Contracted personnel will not have physical access to restricted areas of CalSTRS (e.g., printers providing services off-site and delivering product)
- Contracted personnel will not have access (physical or electronic) to confidential/sensitive data (e.g., lecture style training)

CERTIFICATION OF CONTRACTOR'S EMPLOYEE BACKGROUND INVESTIGATION

Contractor Firm Name ("Contractor"): _____

Contractor, as a condition of providing Services as set forth in the above-referenced Agreement, certifies the following:

1. Contractor has agreed to and will comply with the CalSTRS Contractor Background Investigation Policy, attached and incorporated into the Agreement.
2. Prior to assigning any of Contractor's employees ("Contractor Personnel") to perform the services called for in the Agreement or providing such individuals access to CalSTRS information (the "CalSTRS Assignment"), Contractor will perform a background investigation on such individuals that complies with the CalSTRS Contractor Background Investigation Policy and applicable law ("Background Investigation").
3. Contractor has performed a Background Investigation on those Contractor Personnel identified on page 2 of this exhibit and hereby certifies that such individual(s) is/are qualified and suitable to work on the CalSTRS Assignment.
4. To the extent Contractor intends to assign any additional Contractor Personnel to the CalSTRS Assignment hereafter, Contractor agrees to provide CalSTRS with an updated Certification covering such individual(s) prior to their work on the CalSTRS Assignment.
5. On an annual basis, Contractor agrees to certify, in writing, that it has not received information related to any Contractor Personnel which would justify removing such individual from the CalSTRS Assignment.
6. Contractor has been informed and understands that any violation of this certification may result in the termination of the Agreement, at CalSTRS' election. The termination of the Agreement shall not be construed to limit any remedy CalSTRS might have under applicable law.

I, _____ (printed name), declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed in _____ (city), _____ (state)

on _____.

Authorized Signature

Title

Contractor Personnel

Contractor agrees to conduct a Background Investigation of the following named Contractor Personnel and certify their qualification prior to any CalSTRS Assignment:

- 1.
- 2.
- 3.
- 4.
- 5.

PERSONAL HISTORY STATEMENT FOR

CONTRACTED EMPLOYEE NAME

It is CalSTRS' policy to prevent a conflict of interest that could arise from having employees or contracted employees work on, or have access to, the records and accounts of CalSTRS employees, members, or beneficiaries with whom they have a personal relationship.

A member or beneficiary is: (1) any teacher or other certificated staff member in a California school district kindergarten through community college who is active or retired from such a position; (2) a member of the Cash Balance Program; (3) a member of the Defined Benefits Program; or (4) someone who is a survivor of someone who retired from such a position.

A Personal Relationship, includes, but is not limited to, associations with individuals by: (1) blood, adoption, and guardianship (i.e., mother, father, daughter, son, sister, brother, half-sister, half-brother, grandparents, grandchild, aunt, uncle, niece, nephew, or first cousin); (2) marriage or previous marriage (i.e., current or former spouse, in-laws, stepmother, stepfather, stepson, stepdaughter, stepsister, or stepbrother); (3) domestic partnership and/or cohabitation (i.e., current or former domestic partner or cohabitants, or their relatives); or (4) any other type of romantic relationship (i.e., girlfriend or boyfriend).

Please provide us the name(s) of any individual(s), to the best of your knowledge, to whom you have a personal relationship as defined above, who is currently a member or beneficiary of CalSTRS, a current CalSTRS employee or CalSTRS contractor. Follow the instructions below:

1. Insert your name in the *Contracted Employee Name* space at the top of the page.
2. List the name(s) of persons in the table below for which you have a personal relationship.
3. Place an X next to the name(s) to indicate the applicable relationship category.
4. If you have no relationship(s) as defined above, leave the table below blank.

Name	CalSTRS Employee	CalSTRS Contractor	CalSTRS Member/Beneficiary

Signature

Date

CalSTRS INFORMATION SECURITY AND PRIVACY ADDENDUM

This Information Security and Privacy Addendum (hereinafter, "Addendum") establishes minimum requirements Contractor shall adhere to in order to protect any confidential or sensitive information disclosed to Contractor by CalSTRS in connection with or relating to the parties' agreement (hereinafter, "Agreement"). This Addendum is expressly incorporated into and made a part of such Agreement. All capitalized terms not specifically defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions. For the purposes of this Addendum, the following definitions shall apply:

- a. Contractor: Includes the Contractor, its officers, employees, agents, subcontractors, and anyone directly or indirectly employed, directed or controlled by Contractor.
- b. CalSTRS Information and Information Systems (hereinafter, "CalSTRS Information"): Information that is collected, created, stored, processed, transmitted or disseminated in connection with the negotiation or performance of this Agreement; including Public Information, Confidential Information, Sensitive Information and Personally Identifiable Information. Information Systems denote frameworks of hardware, software, applications, data, processes and personnel that manage, store and transmit information.
- c. Public Information: Information that is not exempt from public disclosure under the provisions of the California Public Records Act (Government Code section 7920.000 et seq.) or other applicable state or federal laws.
- d. Confidential Information: Information that is exempt from public disclosure under the provisions of the California Public Records Act (Government Code section 7920.000 et seq.) or other applicable state or federal laws.
- e. Sensitive Information: Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss or deletion. Sensitive Information may be Public Information or Confidential Information. Sensitive Information is information that requires a higher-than-normal assurance of accuracy and completeness. The key factor for Sensitive Information is integrity.
- f. Personally Identifiable Information: Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, personal telephone number, education, financial matters and medical or employment history. CalSTRS considers personal information confidential unless such information is determined to be a public record.
- g. Incident: An event, confirmed or otherwise, that has been discovered or reported, that actually or imminently jeopardizes the confidentiality, integrity or availability of computers, communication systems, networks, physical or virtual infrastructure,

or information resident thereon. Note: not all Information Security Incidents result in a Data Breach.

- h. Data Breach: A confirmed Incident where CalSTRS Information is adversely affected by events that take place due to unauthorized, malicious actions or by the unintended actions of staff. A breach may or may not be accompanied by an active attack. A 'breach' implies destruction, theft, alteration or dissemination of data to benefit the attacker or harm CalSTRS materially or by reputation.

2. Non-Disclosure

Contractor shall:

- a. Protect CalSTRS Information from unauthorized disclosure as stated in the CalSTRS Confidentiality, Non-Disclosure and Acceptable Use Agreement (ISO 1948).
- b. Not use CalSTRS Information for any purpose other than carrying out the Contractor's duties under the Agreement.
- c. Promptly submit to CalSTRS Compliance Officer (contact information below) all requests for disclosure of CalSTRS Information.

3. Information Security Plan

Contractor shall establish, implement and at all times during the term of the Agreement, maintain administrative, physical and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, integrity and availability of CalSTRS Information (hereinafter, "Information Security Plan"). When requested by CalSTRS, Contractor shall provide a copy of its Information Security Plan to CalSTRS.

Contractor's Information Security Plan shall: (i) comply with applicable state, federal and international laws; (ii) meet or exceed the Federal Information Processing Standards Publication 199 protection levels, and (iii) include each of the Center for Internet Security's Critical Security Controls (available at <https://www.cisecurity.org/critical-controls.cfm>).

4. Information Security Officer

Contractor shall designate an Information Security Officer to oversee its Information Security Plan. The Information Security Officer shall communicate with CalSTRS on security matters relating to this Addendum.

5. CalSTRS Minimum Information Security Requirements

To the extent required by CalSTRS, Contractor shall also comply with any CalSTRS' detailed minimum information security requirements. If the Agreement is amended and CalSTRS has updated its minimum information security requirements since the time of the original Agreement or last amendment, Contractor shall recertify to CalSTRS that it is complying with the minimum information security requirements in effect at the time of the

most recent amendment. Failure of Contractor to recertify that it meets any minimum information security requirements shall be deemed a material breach of the Agreement.

6. Incident Response

- a. Contractor shall report any confirmed or suspected Incident to CalSTRS Information Security Office and CalSTRS IT Service Desk (contact information below), and the CalSTRS business contact with whom the Contractor maintains a working relationship, **immediately** upon discovery and identify a) the nature of the Incident, b) the CalSTRS Information at issue and c) the person(s) involved in the Incident (if known).
- b. Contractor shall undertake immediate remediation measures upon the occurrence of any Incident while preserving all forensic evidence feasible under the circumstances.
- c. Contractor, in consultation with CalSTRS, shall ensure that it complies with California law concerning Data Breach notifications (currently found in California Civil Code §§ 1798.29, 1798.82), as such laws may be amended or modified. CalSTRS shall approve the time, manner and content of any such notifications.
- d. Within ten (10) working days, or at the earliest possible time thereafter, Contractor shall describe any responsive mitigation measures which have been taken (or which are proposed to be taken), and what corrective action Contractor has taken (or plans to take) to prevent future similar Incidents. In addition, Contractor shall provide any related additional information or reports reasonably requested by CalSTRS, a CalSTRS designated third party or law enforcement. In the event Contractor undertakes any investigation of a suspected Incident, it shall keep CalSTRS regularly apprised of its investigatory progress at intervals requested by CalSTRS.
- e. Contractor shall fully cooperate with any investigation conducted by CalSTRS, a CalSTRS designated third party or law enforcement with respect to any suspected Incident involving or relating to Contractor or CalSTRS Information, including (without limitation):
 - i. Immediately applying appropriate resources to assist in the investigation and remedying of the Incident;
 - ii. Preserving and providing all potential forensic evidence relating to the Incident;
 - iii. Promptly designating an individual as the prime contact for any CalSTRS communications or inquiries;
 - iv. Making witnesses and documents immediately available to CalSTRS, a CalSTRS designated third party or law enforcement requests;

v. Providing status reports to CalSTRS on Contractor's response activities.

- f. Contractor shall additionally fully cooperate and make itself available to CalSTRS, a CalSTRS designated third party or law enforcement at no additional cost in order to testify as a witness, or otherwise, in the event of an Incident which relates to Contractor's performance hereunder (or other unauthorized disclosure of CalSTRS Information caused by Contractor) and which results in litigation, governmental investigation(s) or an administrative proceeding(s) by or against CalSTRS (or its directors, officers, agents or employees).

7. Information Security Indemnity

Contractor agrees to indemnify, defend and hold harmless the State of California, CalSTRS, the Teachers' Retirement Board, the Teachers' Retirement Fund and all of the officers, trustees, agents and employees of the foregoing, from and against any and all losses, costs, liabilities, damages or deficiencies, including interest, penalties and attorneys' fees, which 1) arise out of or are due to a breach by Contractor of any of its representations, warranties, covenants or other obligations contained in this Agreement, or 2) are caused by or resulting from Contractor's acts or omissions constituting bad faith, willful misfeasance, negligence or reckless disregard of its duties under this Agreement, or 3) accrue or result to any of Contractor's subcontractors, materialmen, laborers or any other person, firm or corporation furnishing or supplying services, material or supplies in connection with the performance of this Agreement.

8. Contractor's Information Security Representations and Warranties

- a. Contractor warrants that any material information relating to any security Incidents from the past five (5) years has been disclosed to CalSTRS.
- b. Contractor shall disclose any legal or regulatory actions pending against Contractor relating to an Incident, and to Contractor's actual knowledge, also disclose if there are any legal or regulatory actions threatened against Contractor relating to an Incident.
- c. Contractor warrants that there will be no processing, storage or transmission of CalSTRS Information by third parties (fourth parties to CalSTRS) not approved by CalSTRS in writing. Contractor shall direct any approved third party to adhere to the provisions of this Addendum. Contractor will provide copies of its fourth-party risk management policies to CalSTRS upon request.
- d. Contractor represents and warrants that it shall employ or contract with and retain at all times sufficient personnel qualified or paid security service to maintain and execute its Information Security Plan.

9. Cyber Security Insurance

When deemed necessary by CalSTRS, in addition to that insurance required to be carried by Contractor under the Agreement, Contractor agrees to obtain and maintain during the term a policy of insurance that provides coverage for privacy and data security Incidents with policy limits of at least \$1,000,000 (per occurrence) and \$5,000,000 (aggregate). The cost of this additional policy shall be borne by Contractor and the policy shall include coverage for the reasonable cost of investigating and responding to Information Security Incidents.

10. Effect on Related Transactions

The terms of this Addendum shall apply to all contracts, subcontracts and sub-awards, regardless of whether they are for the acquisition of services, goods or commodities. The Contractor shall incorporate the contents of this Addendum into each subcontract or sub-award to its agents, subcontractors, or independent consultants.

11. Amendment

The parties acknowledge that federal and state laws and regulations relating to information security and privacy are rapidly evolving and that amendments to this Addendum may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CalSTRS Information. The parties agree to promptly enter into negotiations concerning an amendment to this Addendum consistent with new standards and requirements imposed by applicable laws and regulations.

12. Interpretation

The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

13. Return or Destruction of CalSTRS Information

Within 30 days of written notice from CalSTRS of the termination, cancellation, expiration or other conclusion of this Addendum, Contractor will return any and all CalSTRS Information (either in original format or a reasonably acceptable human readable format agreed upon in writing by both CalSTRS and Contractor). Contractor will destroy all CalSTRS Information, and both parties will work together in good faith to determine an appropriate timeline and confirmation process for the data destruction. This paragraph will also apply to all CalSTRS Information that is in the possession of Contractor. Contractor will certify in writing to CalSTRS that Contractor has returned any and all CalSTRS Information, or destruction has been completed.

If Contractor believes that return or destruction of the CalSTRS Information is technically impossible or impractical, Contractor shall provide CalSTRS with a written statement of the reason executed under penalty of perjury under the laws of the state of California. If CalSTRS decides that return or destruction is technically impossible or impractical, Contractor will continue to protect the CalSTRS Information in perpetuity in accordance with the terms of this Addendum and under the coverage outlined in Section 9 of this Addendum.

14. Contact Information

To direct communications to the above referenced CalSTRS staff, the Contractor shall initiate contact as indicated herein. CalSTRS 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 Addendum or the Agreement to which it is incorporated.

CalSTRS Compliance Officer	CalSTRS Information and Security Officer	CalSTRS IT Service Desk
Name: Office of the General Counsel Phone: 916-414-1724 Email: compliance@CalSTRS.com	Name: Information Security Office Phone: 916-414-1999 Email: ISO@CalSTRS.com	Name: IT Service Desk Phone: 916-414-HELP Email: TSServiceDesk@CalSTRS.com

This form is intended for external use only

Authorized Representative Name: _____

Organizational Title: _____

Entity Name: _____

By signing this form, I, the 'Authorized Representative,' hereby represent and warrant that I have the authority to act on behalf of the entity, and its employees, hereinafter collectively referred to as the 'Entity,' and that I am duly authorized to enter into and execute such agreements on behalf of the Entity. I further acknowledge that the terms of this agreement are binding upon the Entity.

I also personally agree to abide by the terms and conditions set forth herein and accept personal responsibility for compliance with this agreement. Additionally, I commit to providing the necessary training and education to the Entity regarding the terms, obligations and responsibilities outlined in this agreement.

Furthermore, both the Entity and I acknowledge that we:

- Must ensure the upmost protection of any data, whether it be confidential, sensitive or personally identifiable information, from any unauthorized individuals or parties, without exception, as required by applicable laws, regulations and CalSTRS policies and standards.
- Have a collective responsibility to protect CalSTRS' business data and information.
- Acknowledge that CalSTRS strictly enforces information security.
- Understand that accessing member accounts of family, friends and acquaintances is strictly forbidden.

Any breach of confidentiality, unauthorized access, disclosure or mishandling of such data puts CalSTRS' information at risk, is potentially illegal and may result in disciplinary actions, including but not limited to legal consequences and termination of the associated contract. Protecting CalSTRS' intellectual property from unauthorized access is of paramount importance to the parties involved, and failure to uphold this commitment will be met with strict consequences to maintain the trust and integrity of CalSTRS.

Authorized Representative Name (print)

Signature

Date

We/I agree to protect all confidential, sensitive and personally identifiable information from unauthorized access, disclosure or mishandling including, but not limited to:

- Member account information.
- Claimant and member employer information.
- Information pertaining to individuals that concerns their personal life, or that can serve, directly or indirectly, to identify or describe an individual.
- Confidential and proprietary information belonging to other agencies.
- Employee personnel, medical or other personally identifiable information.

- Methods employed by agencies to safeguard information, including, without limitation, system, network and server configurations.
- All security-related devices, data or information, such as tokens, access cards, User IDs or associated passwords.

We/I agree to protect the foregoing data and information in the following ways:

- Access, inspect, use, store, disclose or modify information *only* to perform official duties.
- Never access, attempt to access, inspect, store, use, disclose or modify information, including my own, for curiosity, personal gain or any non-business-related reason.
- Secure CalSTRS electronic or physical documents containing confidential, sensitive or personal information only in approved CalSTRS storage facilities.
- Video or photographs of non-public areas of CalSTRS are permitted only when taken with CalSTRS issued devices and only with prior authorization from your CalSTRS supervisor or manager and the consent of any individuals involved.
- Video or audio recordings of CalSTRS' personnel or non-public activities are prohibited without prior express written permission from your CalSTRS supervisor or manager and the consent of any individuals involved.
- Comply with all CalSTRS policies, standards and procedures for data and information, including secure transportation, handling, use in generative artificial intelligence, retention and destruction.
- Return all CalSTRS owned devices and immediately cease using User ID and password upon separation from CalSTRS.
- Always lock (Ctrl + Alt + Del, then click 'Lock' or Windows key + L) computer systems if you intend to leave them unattended.

We/I acknowledge acceptable activities are those in accordance with the laws, regulations and policies of the United States Government and the State of California, and consistent with the policies, purpose, goals and mission of CalSTRS, as appropriate to my assigned job duties and responsibilities.

We/I expressly consent to CalSTRS monitoring all our devices and activities used to conduct or discuss CalSTRS business, information, or data and acknowledge that there is no expectation of privacy related to any information including, but not limited to, personal or business email accounts, devices such as computers or phones, access to CalSTRS systems or facilities, CalSTRS networks and servers or any electronic or physical records or data. Any information gathered may become discoverable as evidence in a court of law when relevant to legal proceedings, internal or external investigations and may also be provided pursuant to the California Public Records Act (CPRA).

Authorized Representative Name (print)

Signature

Date

REFERENCE

CalSTRS' Information Security Policy; Civil Code section 1798 et seq; Education Code section 22306; Government Code sections 11019.9 and 7920.000 et seq.; Federal Acquisition Regulation (48 CFR 27.402 Policy); and State Administrative Manual section 5300-5360.1 and 4986-4986.13.

CERTIFICATION

I certify that I have read this document and understand information security is strictly enforced. I certify that unauthorized access, inspection, use, storage, disclosure or modification of confidential, sensitive, non-public or personal information, including my own, or any attempt to engage in, or failure to prevent such acts is prohibited. Noncompliance with this agreement or attempt to circumvent any information security policy, standard, procedure or control puts CalSTRS' information at risk, is potentially illegal and may be grounds for legal action taken against me and the Entity.

Authorized Representative Name (print)

Signature

Date

ASSISTANCE

Contact the CalSTRS Legal Department at (916) 414-1724 if you have questions or need assistance completing the form.



Securing the Financial Future and Sustaining the Trust of California's Educators

CalSTRS MINIMUM INFORMATION SECURITY REQUIREMENTS (MISR)

This orange highlight refers to controls that apply to the Moderate Tier, all controls apply to the High tier.

The CalSTRS Information Security Office (ISO) may request additional controls if minimum requirements cannot be met or sufficiently compensated.

As a state agency, CalSTRS is subject to the California Public Records Act (Division 10 (commencing with Section 7920.000), Title 1, Government Code). Information provided in response to these minimum requirements is a public record, but will be deemed confidential to CalSTRS to the extent your responses are confidential under the Public Records Act. If you have any questions or concerns, please contact ISO.

General	
GEN-1	Contractor certifies that its officers, employees, agents, subcontractors, and anyone directly or indirectly employed, directed or controlled by the Contractor will comply with the CalSTRS information security requirements.
Architecture	
ARC-1	All user access to cloud-based services must be routed through secure access controls and authentication mechanisms to support enforcement of security policies and protection of data.
ARC-2	Systems must implement a layered architecture to physically or logically separate presentation, business logic and data storage.
ARC-3	Multi-tier architectures must enforce network segmentation between layers using firewalls or equivalent access controls.
ARC-4	Network traffic must be controlled using a default deny approach, allowing only authorized inbound and outbound connections necessary for business operations.
Artificial Intelligence (AI)	
AIS-1	Vendors must disclose whether Artificial Intelligence (AI) is used within any infrastructure, services, or operational processes.
AIS-3	Use of AI must be subject to a defined governance process that addresses risk management, security, accountability, and compliance.
AIS-5	AI models may be trained on data provided by the customer, third-party data, or a combination of both. The source and nature of training data must be clearly defined.
AIS-6	Customer data must not be shared externally for AI training or any other purpose.
AIS-7	AI models must not include copyrighted or proprietary material without legal authorization.
AIS-8	AI systems must include human oversight to ensure responsible operation and intervention when needed.
AIS-10	AI models hosted outside the customer's infrastructure must be restricted to authorized data owners or custodians designated by the customer.

AIS-11	A shared responsibility model must be defined for cloud-hosted infrastructure and AI systems, clearly delineating roles for managing data, security, and operational outcomes.
AIS-12	AI systems must undergo rigorous testing and include assurance controls such as data validation, performance testing, integrity monitoring, and transparency in algorithm updates to reduce the risk of unintended behavior.
AIS-14	Organizations must maintain an inventory of Large Language Models (LLMs) and other integrated AI systems, including their purpose, version, and usage context. LLMs must be compatible with applicable security protocols and regulatory requirements.
Audit and Event Logging	
Event and Activity Logging	
AEL-1	Audit logs must capture all authentication events, both successful and unsuccessful, and must include sufficient detail to uniquely identify the user and related activity.
AEL-2	System logs must be formatted for compatibility with centralized logging solutions and must be actively transmitted to an approved log aggregation or SIEM platform.
AEL-3	Access to log data must be restricted to authorized personnel with a defined business need.
AEL-4	Logs must be protected against unauthorized access, including from administrators of the systems that generate the logs, and must only be viewable by individuals with a documented business need.
Availability and Retention	
AEL-5	Audit records must be retained for a minimum of 90 days and made available in a timely manner to support security investigations and regulatory or legal obligations.
AEL-6	Requirements for system and application logging must be defined, documented, and periodically reviewed. Logging capabilities, including resource impacts such as storage, performance, and scalability, must be evaluated when implementing or onboarding systems.
Data Handling and Custody	
DHC-1	Customer data and underlying structures must be logically or physically isolated from other clients and must not be used for general benchmarking, analytics, or marketing purposes.
DHC-2	Customer data must be stored, backed up, and processed only within the continental United States, in accordance with applicable contractual and regulatory requirements.
DHC-3	Upon request or contract termination, all customer data must be returned in either its original format or another mutually agreed, human-readable format. After the customer formally accepts the returned data, the provider must permanently delete all retained copies and provide written confirmation of deletion.
Encryption Standards	
ENC-1	Data must be encrypted using industry-accepted cryptographic algorithms that meet or exceed current security standards.
ENC-2	Data integrity must be ensured using cryptographic methods such as hashing to detect unauthorized modifications and validate authenticity.

ENC-3	Cryptographic keys must be securely stored in encrypted, access-controlled environments to prevent unauthorized access or disclosure.
ENC-4	Cryptographic keys must be retired or replaced prior to expiration or immediately upon suspected compromise.
External Audit and Assurance	
EAA-1	Independent security assessment reports, such as SOC 2, ISO/IEC 27001, or equivalent, must be made available for review upon request.
EAA-2	Independent security assessment reports must be dated within the past 12 months to ensure current control effectiveness.
EAA-3	A documented remediation plan must be in place for any findings identified in SOC 2 or equivalent audit reports.
Identity and Authentication Management	
Account Management and Access Control	
IAM-1	Each user account must be uniquely assigned to a single individual to ensure traceability and accountability.
IAM-2	Access must be managed using role-based access control and separation of duties to align privileges with user responsibilities and reduce risk of misuse.
IAM-3	User access must be limited to only the permissions necessary to perform authorized job functions, following the principle of least privilege.
IAM-4	Guest accounts and accounts without passwords must be disabled to prevent unauthorized access.
IAM-5	Multifactor authentication should be used, where appropriate, to supplement password protections such as when accessing systems remotely or performing high-risk activities.
IAM-6	Group or shared user accounts and passwords must not be used.
Password Policy and Configuration	
IAM-7	Password-based authentication must include a unique user identifier and a corresponding password. User identifiers must not be changed once assigned and must be retained for as long as necessary to meet business, legal, or audit requirements.
IAM-8	Password complexity requirements must enforce a combination of at least three-character types: uppercase letters, lowercase letters, numbers, and special characters.
IAM-9 For systems that support long passwords:	
IAM-9.1	Systems that support long passwords must enforce a minimum password length of 15 characters.
IAM-9.2	Systems that support long passwords must retain history of at least 12 passwords.
IAM-9.3	Systems that support long passwords must limit password age to 730 days.
IAM-9.4	Systems that support long passwords must lock accounts after no more than 5 consecutive invalid login attempts.
IAM-10 For administrative, system and service accounts on systems that can support long passwords:	
IAM-10.1	Administrative, system and service accounts on systems that can support long passwords must enforce a minimum password length of 20 characters?

IAM-10.2	Administrative, system and service accounts on systems that can support long passwords must retain password history for at least 12 cycles.
IAM-10.3	Administrative, system and service accounts on systems that can support long passwords must limit password age to 30 days.
IAM-10.4	Administrative, system and service accounts on systems that can support long passwords must lock accounts after no more than 5 invalid login attempts.
IAM-10.5	Administrative, system and service accounts on systems that can support long passwords should use a centralized solution to enforce password controls consistently across privileged systems.
IAM-11 For systems that cannot support long passwords:	
IAM-11.1	Systems that cannot support long passwords must enforce a minimum password length of 8 characters.
IAM-11.2	Systems that cannot support long passwords must limit password age to 90 days.
IAM-11.3	Systems that cannot support long passwords must retain history of at least 12 cycles.
IAM-11.4	Systems that cannot support long passwords must lock accounts after no more than 5 consecutive invalid login attempts.
IAM-12 For administrative, system and service accounts on systems that cannot support long passwords:	
IAM-12.1	Administrative, system and service accounts on systems that cannot support long passwords must enforce a minimum password length of 8 characters.
IAM-12.2	Administrative, system and service accounts on systems that cannot support long passwords must limit password age to 365 days.
IAM-12.3	Administrative, system and service accounts on systems that cannot support long passwords must retain history of at least 12 cycles.
IAM-12.4	Administrative, system and service accounts on systems that cannot support long passwords must lock accounts after no more than 5 consecutive invalid login attempts.
IAM-13	Default or initial passwords must be changed upon first login to prevent unauthorized access.
IAM-14	Passwords must not contain the user ID or any portion of the associated user's name.
IAM-15	Default passwords on devices must be changed prior to deployment or integration into any production environment.
IAM-16	All accounts, including testing and training accounts, must not use generic passwords. First-time passwords must be uniquely assigned and changed promptly after initial use.
IAM-17	Passwords must not be based on personal information, including names, dates, phone numbers, or addresses.
IAM-18	Passwords for domain administrator, system, and service accounts must be changed when personnel with access to them leave the organization. These passwords must remain confidential and be shared only with the minimum number of administrators necessary for operational support.
IAM-19	Passwords for privileged accounts must be unique for each system or service to prevent credential reuse across environments.
IAM-20	Built-in password policy enforcement mechanisms should be used to support centralized and consistent password management.

IAM-21	New passwords must be sufficiently different from previously used passwords to prevent reuse or predictable variation.
Password Use and Handling	
IAM-22	Passwords must not be embedded in scripts, macros, or other forms of automated code execution.
IAM-23	Passwords must be distributed using secure methods that prevent unauthorized disclosure or alteration.
IAM-24	Passwords must remain confidential and must not be disclosed.
IAM-25	Passwords must not be written down or stored in plain text, whether in physical or digital form.
IAM-26	Password autofill or “remember password” features must not be used, except within an approved password vault or privileged access management (PAM) solution.
Incident Response and Notification	
IRN-1	Confirmed or suspected security incidents must be reported immediately and must disclose, at minimum: the nature of the incident, affected data or systems, individuals involved (if known), mitigation actions taken or proposed, and corrective actions to prevent recurrence.
IRN-2	Relevant event logs associated with any security incident must be retained and made available to support investigation and response.
IRN-3	Additional incident-related information or reports must be provided upon request and must keep impacted parties informed of investigation progress if an investigation is conducted.
IRN-4	Security systems must support endpoint-wide investigative scanning, including RegEx, file, hash, and value search capabilities, along with integrated tools for malicious activity review, tagging, annotation workflows, and hunting for Indicators of Compromise (IOCs) through event analysis.
IRN-5	Security systems must support root cause investigations through integrated forensic capabilities, including user and entity behavior analysis and historical process mapping.
IRN-6	Security systems must provide built-in analysis and reporting tools, as well as the ability to create and customize searches and investigation workflows.
Patches, Hotfixes and Updates	
PHU-1	Security patches classified as high, critical or emergency must be applied to all systems within defined timeframes based on risk and severity.
PHU-2	Patches for infrastructure components such as firewalls, routers, switches, and network appliances must be reviewed at least quarterly. Additional patches must be applied as needed to address high-risk vulnerabilities.
PHU-3	High, critical and emergency patches must be tested and deployed to all endpoints within a timeframe appropriate to the associated risk.
Physical and Environmental Security	
Where appropriate to the organization’s role:	

PES-1	Physical security controls must be implemented, which may include key card/badge access systems.
PES-2	Physical security controls must include access logging, retained for a minimum of 90 days.
PES-3	Physical security controls must include video surveillance with retention for a minimum of 90 days.
PES-4	A 24-hour monitored security system must be in place.
PES-5	On-site security personnel must be provided.
PES-6	Fire detection and protection systems must be implemented and maintained.
PES-7	Secure on-site media destruction must be used for the disposal of physical media containing sensitive information.
Virus Protection	
Detection and Protection Capabilities	
VIP-1	Malware protection must be deployed on all endpoints and must include real-time, on-agent detection and prevention using both signature-based and behavior-based techniques. Solutions must be capable of identifying and blocking known and emerging threats, including fileless attacks, memory-based exploits, indicators of compromise, and zero-day vulnerabilities.
VIP-2	Malware protection tools must support integration with security monitoring and response systems.
VIP-3	Malware protection systems must provide near real-time visibility into endpoint inventory and application versions through centralized reporting.
VIP-4	Malware protection systems must support current and updated releases of Windows, Linux, and Mac operating systems, and be continuously maintained by the vendor to support future platform versions.
Endpoint Agent Configuration	
VIP-5	Endpoint protection agents must be protected from unauthorized disablement or uninstallation through password protection or equivalent controls.
VIP-6	Endpoint protection systems must support centralized software distribution for updates or integrate with existing enterprise distribution tools.
Investigative Support Capabilities	
VIP-7	Security systems must maintain a historical timeline of key endpoint activities across monitored devices, which may include file, registry, network, driver, and execution events, along with indicators of business impact such as data loss or fraud.
Web Application Security	
Secure Configuration and Server Hardening	
WAS-1	Web applications must redirect all HTTP traffic to HTTPS to ensure secure, encrypted communication.
WAS-2	Web applications must use TLS version 1.2 or higher to ensure secure communication.
WAS-3	Unused or unnecessary files must be removed from web servers to reduce attack surface.

WAS-4	Development or debugging code must not be present on production systems.
WAS-5	Secrets such as API keys, credentials, tokens, and certificates must not be stored in source code or configuration files.
WAS-6	Static HTML pages must not contain scripting or executable content to reduce exposure to client-side attacks.
WAS-7	Directory listing and directory browsing must be disabled on all production web servers.
WAS-8	Web applications must use DNS aliases instead of direct IP access to abstract infrastructure details and support secure naming.
WAS-9	Web applications must implement HTTP response headers that enforce secure transport and content-type protections, such as Strict-Transport-Security and X-Content-Type-Options.
WAS-10	Web applications must implement security headers that restrict content execution and control browser behavior, such as Referrer-Policy, Content-Security-Policy, and X-Frame-Options.
Authentication and Identity Management	
WAS-11	Authentication credentials must be encrypted in transit using secure protocols to prevent interception or unauthorized access.
WAS-12	Authentication should be managed through a centralized or federated identity service to support consistent access control across applications.
WAS-13	Web application components must mutually authenticate when communicating across backend services to ensure trust and prevent impersonation.
WAS-14	Web applications must support strong authentication mechanisms such as multi-factor authentication to reduce the risk of unauthorized access.
WAS-15	Access rights for web applications, including user roles and server or service accounts, must follow the principle of least privilege.
WAS-16	Web applications must enforce strong password policies aligned with current security best practices.
WAS-17	Authentication error messages must be generic and must not reveal whether a username or password is valid.
Secure Coding and Configuration	
WAS-18	Web applications must not include hard-coded infrastructure details such as database names, usernames, or hostnames in source code.
Input Validation and Error Handling	
WAS-19	Web applications must perform data validation on both username and password input fields to prevent injection and other input-based attacks.
WAS-20	Web applications must validate and sanitize all user input on both the client and server side to prevent injection, data tampering, and other input-based attacks.
Session Management and Protection	
WAS-21	Session identifiers and cookies must be transmitted over encrypted channels using secure protocols such as TLS and must be validated to ensure authenticity.
WAS-22	Web applications must enforce session management for authentication events, including issuing a new session identifier upon successful login.
WAS-23	Authentication sessions must use secure, cryptographically random tokens to prevent session prediction or fixation.

WAS-24	Authenticated session identifiers must be encrypted in transit to prevent interception or misuse.
WAS-25	Web applications must invalidate authentication sessions upon logout to prevent reuse or unauthorized access.
WAS-26	Web applications must enforce session expiration and idle timeout limits, particularly for applications that process or store personal or sensitive data.
WAS-27	Web applications must require users to re-authenticate before performing sensitive actions, such as modifying personal or account-related information.