Microsoft 365 Implementation Services

Request for Proposal

February 2021

Orange County Employees Retirement System (OCERS)
2223 E. Wellington Avenue, Suite 100
Santa Ana, CA 92701 USA
(714)-558-6200
http://www.ocers.org

Contents

Section 1: Introduction 3
Section 2: Background 3
Section 3: Scope of Services 3
Section 4: General Conditions 4
Section 5: Point of Contact 4
Section 6: Response to Request for Proposal 5
Section 7: Proposal Requirements 6
Section 8: Evaluation Criteria 7
Section 9: Non-Discrimination Requirement 7
Section 10: Notice Regarding the California Public Records Act and the Brown Act 7
Section 11: Contract Negotiations 8
Section 12: Reservations by OCERS 9
Exhibit A: Intent to Respond 10
Exhibit B: Scope of Services 11
Exhibit C: Minimum Qualifications Criteria 26
Exhibit D: Proposal Cover Page and Checklist 27

Section 1: Introduction

The Orange County Employees Retirement System ("OCERS") is requesting proposals from qualified firms interested in providing Microsoft 365 implementation services.

Those who wish to be considered must submit their completed proposal by **5:00 p.m., PT,** *March 26, 2021.* Specific instructions for proposal submissions are contained in Section 7 of this RFP.

Questions about this RFP must be submitted in writing by **5:00 pm, PT,** *March 10, 2021* to Jim Doezie, Contracts, Risk & Performance Administrator, by email at jdoezie@ocers.org.

Intent to Respond

If your firm chooses to respond to this RFP, please submit the "Intent to Respond," attached as Exhibit "A", via email to Jim Doezie, by 5:00 p.m., PT, March 10, 2021. Failure to submit your Intent to Respond may disqualify your firm from submitting a response to this RFP.

Section 2: Background

OCERS was established in 1945 under the provisions of the County Employees Retirement Law of 1937, and provides members with retirement, disability, death, and cost-of-living benefits. There are approximately 46,000 members served by OCERS, of which over 19,000 are retirees. OCERS is governed by a nine-member Board of Retirement ("Board") which has plenary authority and fiduciary responsibility for investment of moneys and administration of the retirement system. OCERS has over ninety employees and the Board appoints a Chief Executive Officer who is responsible for the management of the agency. For additional information about OCERS, please refer to the OCERS website at ocers.org.

Section 3: Scope of Services

The detailed scope of services for this engagement is outlined in the attached Exhibit "B" ("Scope of Services"). The primary objective is to provide OCERS with Microsoft 365 implementation services.

The firm selected for this engagement will be expected to meet requirements that include, but are not limited to, the following:

1. The firm must have all necessary permits and licenses to perform the requested services and must be bonded where applicable.

2. Minimum insurance coverage must include the following items, and proof of such insurance must be provided to OCERS prior to the commencement of work, on an annual basis, and upon request:
    - Commercial General Liability: $2M per occurrence, $2M aggregate
    - Automobile Liability: $1M per occurrence, $2M aggregate
    - Workers Compensation: $1M per occurrence, $1M aggregate
    - Umbrella Liability: $8M per occurrence, $8M aggregate
    - *Professional Liability*: $2M per occurrence, $3M aggregate
    - *Cyber Security Insurance*: $2M per occurrence, $5M aggregate
    - *Fidelity Insurance*: $5M per occurrence
    - *Pollution & Remediation Legal Liability: $5M per occurrence, $25M aggregate*

    OCERS must be listed as an additional insured on the above policies.

3. The firm shall provide all personnel, equipment, tools, materials, vehicles, supervision, and other items and services necessary to perform all services, tasks, and functions as requested in this RFP.

4. The initial term of the contract awarded pursuant to this RFP will be for a three period, with OCERS retaining the option to renew the contract, on an annual basis, for up to an additional three (3) years.

5. All work under the contract awarded shall be performed and all equipment furnished or installed in accordance with applicable safety codes, ordinances, and other regulations, including the regulations of the State of California, Division of Industrial Safety and the provisions of the California Labor Code, the Occupational Safety and Health Act of 1970, the California Occupational Health and Safety Act.

6. Minimum Qualifications
   All respondents are required to sign and return the "Minimum Qualifications Certification," attached as Exhibit "C."

Section 4: General Conditions

All terms, conditions, requirements, and procedures included in this RFP must be met for a proposal to be qualified. A proposal that fails to meet any material term, condition, requirement, or procedure of this RFP may be disqualified. OCERS reserves the right to waive or permit cure of non-material errors or omissions. OCERS reserves the right to modify, amend, or cancel the terms of this RFP at any time.

OCERS may modify this RFP prior to the date fixed for submission of a proposal by posting, mailing, emailing or faxing an addendum to the respondents known to be interested in submitting a proposal. Failure of a respondent to receive or acknowledge receipt of any addendum shall not relieve the respondent of the responsibility for complying with the terms thereof.

A respondent's proposal shall constitute an irrevocable offer for the 120 days following the deadline for submission of proposals. Reference to a certain number of days in this RFP shall mean business days unless otherwise specified.

All proposals submitted in response to this RFP will become the exclusive property of OCERS. Proposals will not be returned to respondents.

By submitting a proposal, the respondent acknowledges that it has read this RFP, understands it, and agrees to be bound by its requirements unless clearly and specifically noted in the proposal submitted.

Section 5: Point of Contact

A quiet period will be in effect from the date of issuance of this RFP until announcement of the selection of a firm or firms under this RFP. During the quiet period, respondents are not permitted to communicate with any OCERS staff member or Board Member regarding this RFP except through the Point of Contact named herein. Respondents violating this quiet period may be disqualified at OCERS' discretion. Respondents having current business with OCERS must limit their communications to the subject of such business.

OCERS' normal business hours of operations are from 08:00 to 17:00 Monday through Friday, except for federal and state holidays.

The Point of Contact for all matters relating to this RFP is:	
Name:	Jim Doezie
Title:	Contracts, Risk & Performance Administrator
Address:	OCERS 2223 E Wellington Ave., Suite 100 Santa Ana, CA 92701
Telephone:	(714) 569-4884
Email:	jdoezie@ocers.org
OCERS Website:	www.ocers.org
Status:	See the OCERS website for status of the RFP and announcements. These items can also be found here: https://www.ocers.org/request-proposal

Section 6: Response to Request for Proposal

Proposals must be submitted to the Point of Contact identified in Section 5 and delivered by the due date and time stated below in the RFP Schedule.

OCERS will accept electronic, paper, or both types of submissions. Proposals may be submitted electronically in Microsoft Word or Adobe Acrobat PDF format to the email address noted in Section 5. Submission may also be made by mailing a USB flash drive with the electronic files, or a paper copy to the mailing address noted in Section 5. If paper copies are submitted, two (2) copies must be submitted.

RFP Schedule

The following timetable constitutes a tentative schedule for this RFP process. OCERS reserves the right to modify this schedule at any time.

Deliverable	Date	Time
Release of RFP	Thursday, February 25, 2021	5:00 pm, PT
Intent to Respond Deadline **RFP Questions Deadline**	Wednesday, March 10, 2021	5:00 pm, PT
RFP Answers Posted	Friday, March 12, 2021	5:00 pm, PT
RFP Submission Deadline	Friday, March 26, 2021	5:00 pm, PT
OCERS Review of RFP Submissions	Tuesday, March 30, 2021	5:00 pm, PT
Selection of Finalists	Wednesday, March 31, 2021	5:00 pm, PT

Interviews of Finalists	To be determined – First week of April (tentative)
Service Award [or recommendation to the Board]	To be determined once a vendor has been selected

Section 7: Proposal Requirements

Proposals must include the following information:

1. The "Minimum Qualifications Certification," attached as Exhibit "C."
2. The "Proposal Cover Page and Check List," attached as Exhibit "D."
3. An executive summary that provides the respondent's background, experience, and other qualifications to provide the services included in the Scope of Services.
4. A description of the respondent including:
    a. Brief history, including year the respondent firm was formed.
    b. Ownership structure.
    c. Office locations.
    d. Organization chart.
    e. Number of employees.
    f. Annual revenues.
    g. Scope of services offered.
    h. Respondent's specialties, strengths, and limitations.
    i. The average retention rate (years of service) of the firm's other clients?
5. The names and qualifications of fully trained and qualified staff that will be assigned to OCERS work, including a detailed profile of each person's background and relevant individual experience.
6. At least three (3) references for which the respondent has provided services similar to those included in the Scope of Services. Please include for each reference the individual point of contact, a summary of the work performed, and the length of time the respondent provided each service.
7. Copies of any pertinent licenses required to deliver respondent's product or service (e.g., business license).
8. A copy of respondent's standard professional services contract.
9. A pricing proposal accompanied by an explanation of the pricing proposal for the scope of work be requested including pricing of fees and costs, billing practices, and payment terms that would apply. OCERS does not place any limits on the approach to pricing and is open to presentation of more than one pricing alternative for the scope of work, or portions of it. This section of the response should include an explanation as to how the pricing approach(es) will be managed to provide the best value to OCERS. The respondent should represent that the pricing offered to OCERS is, and will remain, equivalent to or better than that provided to other public pension fund or should provide an explanation as to why this representation cannot be provided. All pricing proposals should be "best and final," although OCERS reserves the right to negotiate on pricing.

10. An explanation of all actual or potential conflicts of interest that the respondent may have in contracting with OCERS.
11. A description of all past, pending, or threatened litigation, including malpractice claims, administrative, state ethics, disciplinary proceedings, and other claims against respondent and/or any of the individuals proposed to provide services to OCERS.
12. Any other information that the respondent deems relevant to OCERS' selection process.

Section 8: Evaluation Criteria

Responses will be evaluated based upon the following:

1. Experience and reputation of the respondent.
2. Quality of the team proposed to provide services to OCERS, including staffing depth, experience, turnover, and compensation.
3. Pricing and value.
4. Delivery and payment terms.
5. Compliance with technical standards contained in this RFP.
6. The organization, completeness, and quality of the proposal.
7. Information provided by references.
8. Other factors OCERS determines to be relevant.

The factors will be considered as a whole, without a specific weighting.

OCERS may require one or more interviews with or personal presentations by finalists to be conducted with staff, Board Members, and/or the entire Board of Retirement.

If the information in the proposal is deemed to be insufficient for evaluation, OCERS may request additional information or reject the proposal outright at OCERS' sole discretion. False, incomplete, or unresponsive statements in connection with a proposal may result in rejection of the proposal.

Section 9: Non-Discrimination Requirement

By submitting a proposal, the respondent represents that it and its subsidiaries do not and will not discriminate against any employee or applicant for employment on the basis of race, religion, color, national origin, ethnic group identification, mental disability, physical disability, medical condition, genetic information, marital status, ancestry, sex, gender, sexual orientation, gender identity, gender expression, age, or military and veteran status.

Section 10: Notice Regarding the California Public Records Act and the Brown Act

The information submitted in response to this RFP will be subject to public disclosure pursuant to the California Public Records Act (California Government Code Section 6250, et. seq., the "Act"). The Act provides generally that all records relating to a public agency's business are open to public inspection and copying unless specifically exempted under one of several exemptions set forth in the Act. If a respondent believes any

portion of its proposal is exempt from public disclosure or discussion under the Act, the respondent must provide a full explanation and mark such portion "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY," and make it readily separable from the balance of the response. Proposals marked "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY" in their entirety will not be honored, and OCERS will not deny public disclosure of all or any portion of proposals so marked.

By submitting a proposal with material marked "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY," a respondent represents it has a good faith belief that the material is exempt from disclosure under the Act; however, such designations will not necessarily be conclusive, and a respondent may be required to justify in writing why such material should not be disclosed by OCERS under the Act. Fee and pricing proposals are not considered "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY".

If OCERS receives a request pursuant to the Act for materials that a respondent has marked "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY," and if OCERS agrees that the material requested is not subject to disclosure under the Act, OCERS will either notify the respondent so that it can seek a protective order at its own cost and expense, or OCERS will deny disclosure of those materials. OCERS will not be held liable, however, for inadvertent disclosure of such materials, data, and information or for disclosure of such materials if deemed appropriate in OCERS' sole discretion. OCERS retains the right to disclose all information provided by a respondent.

If OCERS denies public disclosure of any materials designated as "TRADE SECRETS," "CONFIDENTIAL," or "PROPRIETARY", the respondent agrees to reimburse OCERS for, and to indemnify, defend and hold harmless OCERS, its Boards, officers, fiduciaries, employees, and agents from and against:

1. Any and all claims, damages, losses, liabilities, suits, judgments, fines, penalties, costs, and expenses, including, without limitation, attorneys' fees, expenses, and court costs of any nature whatsoever (collectively, "Claims") arising from or relating to OCERS' non-disclosure of any such designated portions of a proposal; and
2. Any and all Claims arising from or relating to OCERS' public disclosure of any such designated portions of a proposal if OCERS determines disclosure is required by law, or if disclosure is ordered by a court of competent jurisdiction.

Section 11: Contract Negotiations

OCERS will propose a contract to the successful respondent, which will contain such terms as OCERS, in its sole discretion, may require. In addition, the selected firm will agree that this RFP and the firm's proposal will be incorporated by reference into any resulting contract.

This RFP is not an offer to contract. Acceptance of a proposal neither commits OCERS to award a contract to any respondent, nor does it limit OCERS' right to negotiate the terms of a contract in OCERS' best interest, including the addition of terms not mentioned in this RFP. The final contract must, among other terms and conditions required by OCERS, allow OCERS to terminate the contract a) for OCERS' convenience, b) if funds are not appropriated for the services to be provided, or c) for default.

The general form of the contract OCERS intends to use is included as Exhibit "B" ("OCERS Services Agreement"). OCERS reserves the right to make changes to the contract prior to execution, including material changes. The final Scope of Services to be included in the contract will be determined at the conclusion of the RFP process.

By submitting a proposal without comment on the OCERS Services Agreement, respondent will be deemed to have agreed to each term in the OCERS Services Agreement, and to not seek any modifications to it. If respondent objects to any term in the OCERS Services Agreement or wishes to modify or add terms to the OCERS Services Agreement, the proposal must identify each objection and propose language for each modification and additional term sought. A rationale should be included for each objection, modification, or addition.

Section 12: Reservations by OCERS

In addition to the other provisions of this RFP, OCERS reserves the right to:

1. Cancel or modify this RFP, in whole or in part, at any time.
2. Make such investigation as it deems necessary to determine the respondent's ability to furnish the required services, and the respondent agrees to furnish all such information for this purpose as OCERS may request.
3. Reject the proposal of any respondent who is not currently in a position to perform the contract, or who has previously failed to perform similar contracts properly, or in a timely manner, or for any other reason in OCERS' sole discretion.
4. Waive irregularities, to negotiate in any manner necessary to best serve the public interest, and to make a whole award, multiple awards, a partial award, or no award.
5. Award a contract, if at all, to the firm which will provide the best match to the requirements of the RFP and the service needs of OCERS in OCERS' sole discretion, which may not be the proposal offering the lowest fees.
6. Request additional documentation or information from respondents, which may vary by respondent. OCERS may ask questions of any respondent to seek clarification of a proposal or to ensure the respondent understands the scope of the work or other terms of the RFP.
7. Reject any or all proposals submitted in response to this RFP.
8. Choose to not enter into an agreement with any of the respondents to this RFP or negotiate for the services described in this RFP with a party that did not submit a proposal.
9. Determine the extent, without limitation, to which the services of a successful respondent are or are not actually utilized.
10. Defer selection of a bidder to a time of OCERS' choosing.
11. Consider information about a respondent other than, and in addition to, that submitted by the respondent.

Exhibit A: Intent to Respond

If you choose to submit a proposal in response to this RFP please submit this Intent to Respond to Jim Doezie via email no later than 5:00 p.m., PT, Wednesday March 10, 2021**.** Failure to submit your Intent to Respond may disqualify your firm from submitting a proposal.

OCERS' responses to written requests for clarification or additional information will be provided to all firms that have submitted an Intent to Respond.

Intent to Respond

To: Jim Doezie	**From:**
Co.: OCERS	**Title:**
	Co.:
Phone: (714) 569-4884	**Phone:**
Email: jdoezie@ocers.org	**Email:**
Re: Intent to Respond	**Date:**

Our firm intends to submit a response for OCERS' RFP for Microsoft 365 Implementation services.

Please forward inquiries to the following contact:

Name:

Title:

Company:

Mailing Address:

Telephone:

Facsimile:

Email Address:

Exhibit B: Scope of Services

Current Licensing

OCERS has a current and active Microsoft 365 E5 licenses and Microsoft Software Assurance contract for our Windows, Exchange and other Windows licenses.

Current State

OCERS is currently using a hybrid environment consisting of on premise Active Directory synchronized to Microsoft 365. Basic tenant setup is complete but no applications or services are in use other than Intune.

Approximate counts:

Organization:

- 100 - Persons (OCERS staff and Contractors)
- 1 - Physical Location
- 2 - Co-located data centers

Microsoft Windows:

- 75 – Microsoft Windows Servers
- 200 - Microsoft Windows Workstations (Desktops, laptops and tablets)
- 45 - Mobile Devices (iPhone, Android and other devices)

Microsoft Exchange:

- 150- Mailboxes
    - 110 - User Mailboxes
    - 10 - Shared
    - 15 - Service Mailboxes
    - 16 - Resource (Rooms and Calendars)
- 65 - Distribution Lists
- 25 - External Contacts

SharePoint on-prem solution includes SharePoint App, Web, SQL and MOO servers

Exchange on-prem solution include DAG configuration distributed between co-location sites.

Desired Future State (Phase 1)

OCERS is seeking to implement the various applications, features, and functions of Microsoft 365 as noted in the “Requested Services (Phase 1)” section below. This encompasses the following:

- Azure AD
- Office 365 Application Suite
- Exchange Online
- SharePoint Online (potentially in hybrid configuration with on premise SharePoint)

- Microsoft Teams
- Microsoft Endpoint Manager (Intune)
- Enterprise Mobility + Security
- Security best practices for Microsoft 365

Integration with Existing Systems

OCERS currently has (or is in the process of obtaining) systems that may require integration with Microsoft 365. These systems include:

- 3rd Party Cloud Based Secure Email Gateway (SEG) Solution (existing)
- 3rd Party Cloud Based Single Sign-On (SSO) and Multifactor Authentication (MFA) Solution (existing)
- 3rd Party Cloud Based Security Information and Event Management (SIEM) Solution (existing)
- 3rd Party Cloud Based Privileged Access Management (PAM) Solution (in progress)
- Explore Federated Authentication (B2B) with the County of Orange

Recommendation and Implementation of New Systems

As part of the Phase 1 project, OCERS is seeking assistance from respondent vendors to identify, recommend, and possibly implement the following types of systems that will need to be integrated with Microsoft 365:

- Cloud Access Security Broker (CASB) Solution
- Public Cloud Backup Solutions

Requested Services (Phase 1)

The remaining items listed below in this section of Appendix B encompass the scope of work and services required for this engagement.

Note: Items in italics have already been partially or fully implemented. For these items, as part of the Phase 1 project, we are requesting the respondent organization to review/validate our current configuration and recommend/implement changes as necessary.

Microsoft 365 Readiness Assessment, Onsite Discovery, and Planning

- Evaluate current systems to gather and capture information about existing infrastructure
- Evaluate existing custom applications and recommended migration path
- Evaluate existing data reporting environment (SSRS / Power BI) and recommended migration path
- Evaluate and propose solution for hybrid SharePoint configuration
- Identify potential challenges in the migration and propose solutions
- Recommend and execute a solid communications and training plan for end users
- Prepare and provide end user documentation for the new Microsoft 365 environment
- Develop and document migration plan for rollout of additional Microsoft 365 Services

Plan and Provision Office 365

- ***Provision an Office 365 tenant***
    - *Create an Office 365 tenant*

    - *Add a custom domain for Office 365*
    - *Plan DNS zones for custom domains*
    - *Configure DNS records for custom domains*
    - Manage feature updates
- **Plan the deployment**
    - Gather customer requirements
    - Identify customer constraints
    - Identify pilot users
    - Evaluate the pilot deployment
    - Plan the production deployment
    - Review of deployment tools
    - Determine if Microsoft FastTrack will be used for Office 365 onboarding

Office 365 Users and Groups

- **Managing user accounts and licenses**
    - Create user accounts
    - Manage user licenses
    - Manage user accounts
    - Review deleting and recovering user accounts
- **Managing passwords and authentication**
    - Configure password policy options
    - Configure self-service password management
    - Plan password policies and authentication
    - Configure and enable multi-factor authentication
    - Enable Modern Authentication across all services
    - Block Legacy Authentication (through Conditional Access Policies)
- **Managing security groups in Office 365**
    - Create and configure groups
    - Delete groups
- **Configuring administrative access**
    - Review Office 365 administrator roles
    - Assign administrator roles
    - Plan delegated administration

Configure Client Connectivity to Microsoft Office 365

- **Plan for Office 365 clients**
    - Determine which clients will be supported for Office 365 (Windows, Mac, mobile)
    - Determine support for Office Online
- **Plan connectivity for Office 365 clients**
    - Review requirements for network infrastructure
    - Review requirements for network bandwidth
    - Determine if Autodiscover will be implemented
    - Configure Autodiscover (if applicable)
- **Configure connectivity for Office 365 clients**
    - Configure Outlook

- Configure client access to Office Online (if applicable)
- Configure the OneDrive for Business client
- Configure mobile devices

Plan and Configure Directory Synchronization

- **Plan and prepare for directory synchronization**
  - *Plan directory synchronization*
  - *Review prerequisites for directory synchronization*
  - *Prepare for directory synchronization*
  - *Configure tenant for directory synchronization*
- **Implement directory synchronization using Azure AD Connect**
  - *Review Azure AD Connect requirements*
  - *Review Azure AD Connect express synchronization settings*
  - Review Azure AD Connect customized synchronization (if applicable)
  - Review Azure AD Connect Health
- **Manage Office 365 identities with directory synchronization**
  - Review managing users with directory synchronization
  - Review managing groups with directory synchronization
  - Modify directory synchronization (as needed)
  - Monitor directory synchronization
  - Troubleshooting directory synchronization (as needed)

Plan and Deploy Office 365 Client App

- **Review Office 365 Client App**
  - Review of Office 365 Client App
  - Review Office 365 Client App licensing and activation
  - Review Office 365 Client App deployment
  - Review Office 365 Client App update branches
- **Plan and manage Office 365 Client App deployment**
  - Plan for Office 365 Client App deployment
  - Determine deployment type (user-driven or centralized)
  - Manage deployment channels
  - Review and customize Office Deployment Tool (if applicable)
  - Manage and deploy Office 365 Client App with Group Policy
  - Manage Office 365 Client App updates
- **Office Telemetry and reporting**
  - Determine if Office Telemetry should be installed and configured
  - Deploy and configure Office Telemetry (if needed)

Plan and Manage Exchange Online Recipients and Permissions

- **Plan Exchange Online deployment**
  - Review Exchange Online features
  - Review Exchange Online subscription options
  - Plan Exchange Online implementation

    - Review Administration of Exchange Online
- **Manage Exchange Online recipients**
    - Manage Exchange Online mailboxes
    - Configure email addresses
    - Configure distribution groups
    - Configure resources
    - Configure shared mailboxes
    - Configure contacts
    - Bulk importing contacts (if applicable)
    - Configure mail users
- **Plan and Configure Exchange Online Permissions**
    - Plan for Exchange Online admin roles
    - Manage administrative permissions with admin roles
    - Review and configure user roles
    - Disable Calendar sharing with external users

Plan and Configure Exchange Online Services

- **Plan and configure email flow in Office 365**
    - Review email flow in Office 365 (including 3rd party email security service)
    - Configure accepted and remote domains
    - Plan and configure connectors
    - Plan and configure transport rules
    - Plan and configure journal rules
    - Plan and configure client access rules
    - Plan message flow for Office 365
    - Configure external mail flow for partners
    - Review tracking message flow by using message trace
    - Setup and configure on premise SMTP relay
    - Prevent auto-forwarding of emails
- **Plan and configure email protection in Office 365**
    - Review and plan for Exchange Online Protection (EOP)
    - Configure the malware filter
    - Configure the connection filter
    - Configure the spam filter
    - Manage message quarantines
    - Configure Exchange Online Protection reports
    - Integrate EOP with on-premises Exchange servers (if applicable)
    - Configure email protection
    - Configure Advanced Threat Protection
    - Enable MailTips
    - Review SPF, DKIM, DMARC settings and policies
- **Plan and configure client access policies**
    - Configure policies for Outlook on the web
    - Configure access only for authorized devices (prohibit personal devices)
    - Configure access for mobile devices

    - Configure mailbox policies for mobile devices
- **Migrate to Exchange Online**
    - Review options for migrating to Exchange Online
    - Select an option and plan for migration
    - Execute migration

Plan and Configure SharePoint Online

- **Configure SharePoint Online services**
    - Configure SharePoint Online settings
    - Configure SharePoint Online user profiles
    - Add SharePoint Online apps (as needed)
    - Configuring Office 365 Video (as needed)
- **Plan and configure SharePoint Online site collections**
    - Review site collections
    - Review default site collections
    - Plan site collections
    - Create site collections
    - Configure site collections
    - Review common errors and best practices
- **Plan and configure external user sharing**
    - Determine if external user sharing is required/appropriate
    - Understand considerations for using external user sharing
    - Configure external user sharing (if applicable)
    - Review sharing documents and auditing shared access (if applicable)
    - Review how to remove external user sharing
    - Review common errors and best practices

Plan and Configure Reporting and Power BI

- **Configure SQL Reporting Services**
    - Configure SQL Reporting settings
    - Develop migration plan
    - Configure access control
    - Install Azure Data Gateway connector

Plan and Configure OneDrive for Business

- **Plan and configure OneDrive for Business**
    - Review of OneDrive for Business
    - Review OneDrive for Business collaboration features
    - Review using the OneDrive for Business admin center
    - Review managing OneDrive for Business
    - Plan a OneDrive for Business implementation
    - Perform OneDrive for Business client configuration and synchronization
    - Migrate files to OneDrive for Business
    - Configure defaults for sharing including organization wide expirations

Plan and Configure Security and Compliance in Office 365

- **Review the security and compliance features in Office 365**
  - Review security considerations when planning an Office 365 implementation
  - Review compliance and security features in Office 365
  - Review the Security & Compliance Center for Office 365
  - Configure permissions in the Security & Compliance Center
  - Review advanced security and compliance features in Office 365
  - Prevent third party integrated application access
  - Review the need for and deploy an on premise certificate authority (if applicable)
- **Plan and configure Azure Information Protection in Office 365**
  - Review Azure Information Protection in Office 365
  - Planning Azure Information Protection integration with Office 365 (if applicable)
  - Configuring Azure Information Protection integration (if applicable)
- **Configure the compliance features in Office 365**
  - Configure archive mailboxes
  - Configure retention tags and policies in Exchange Online
  - Configure retention tags and policies in SharePoint Online
  - Configure retention tags and policies in OneDrive
  - Configure retention in Security & Compliance Center
  - Configure DLP policies for email in Exchange Online
  - Create DLP policies in Security & Compliance Center
  - Configure compliance search and Office 365 Advanced eDiscovery
  - Configure audit reports

Monitoring and Troubleshooting Microsoft Office 365

- **Troubleshooting Office 365**
  - Review Office 365 troubleshooting
  - Review the Microsoft Remote Connectivity Analyzer
  - Review the Microsoft Office 365 Support and Recovery Assistant tool
  - Review message tracking tools
  - Review hybrid environment free/busy troubleshooter (if applicable)
- **Monitoring Office 365 service health**
  - Review service health information in the Office 365 dashboard
  - Review and configure Office 365 auditing reports
  - Review and configure Office 365 mail and protection reports

Plan and Configure Identity Federation

- **Plan an AD FS deployment (if applicable)**
  - Review AD FS requirements
  - Review AD FS server roles
  - Plan an AD FS deployment for Office 365
  - Plan a highly available AD FS deployment
  - Perform capacity planning

- **Deploy AD FS for identity federation with Office 365 (if applicable)**
    - Install and configure AD FS
    - Install and configure AD FS proxy
    - Install and configure Web Application Proxy for AD FS
    - Configure AD FS using Azure AD Connect
    - Configure AD FS for federation with Office 365
    - Convert the Office365 tenant to federated authentication
    - Verify SSO
    - Review temporary fall back to password synchronization
- **Planning and implementing hybrid solutions (if applicable)**
    - Review of Exchange Server hybrid deployment
    - Configure Exchange Server hybrid deployment
    - Review of SharePoint Server hybrid deployment
    - Configure SharePoint Server deployment

Implement Microsoft 365 Identity and Access

- **User and Group Security**
    - **Identity and Access Management**
        - Establish Identity governance process
        - Review integration with existing Single Sign-On / Multifactor Authentication solution
    - **User Accounts in Microsoft 365**
        - Review of User Identities
        - Review creation of User Accounts
        - Review management of User Accounts and Licenses
        - Review removing and recovering User Accounts
    - **Administrator Roles and Security Groups in Microsoft 365**
        - Review and configure Administrator Roles in Microsoft 365
        - Review and configure Groups in Microsoft 365
        - Review, configure and implement Privileged Identity Management (PIM) in Azure AD
        - Configure auditing for Privileged Identity Management (PIM)
    - **Password Management in Microsoft 365**
        - Plan Password Policies and Authentication
        - Implement Multi-factor Authentication (review potential integration with existing MFA solution
        - Plan and Implement Self-service Password Management (if applicable)
        - Plan, configure and implement Windows Hello for Business
        - Perform Azure Active Directory Access Reviews
        - Review Azure Active Directory Security Defaults
    - **Azure AD Identity Protection**
        - Review Azure Identity Protection
        - Enable Azure Identity Protection
        - Review Detecting Vulnerabilities and Risk Events
        - Review how to conduct an Investigation
- **Identity Synchronization**
    - **Review Identity Synchronization**
        - Review Microsoft 365 Authentication Options

        - Review Microsoft 365 Provisioning Options
    - **Plan for Azure AD Connect**
        - Plan Directory Synchronization
        - Plan for Azure AD Connect
        - Plan Azure AD Connect pass-through authentication (if applicable)
    - **Implementing Azure AD Connect**
        - Configure Azure AD Connect Prerequisites
        - Setup Azure AD Connect
        - Review Azure AD Connect Health
    - **Managing Synchronized Identities**
        - Manage Users with Directory Synchronization
        - Manage Groups with Directory Synchronization
        - Review Azure AD Connect Sync Security Groups
        - Review Troubleshooting Directory Synchronization
    - **Introduction to Federated Identities**
        - Review Claims-based Authentication and Federated Trusts
        - Review Active Directory Federation Services (if applicable)
        - Review Single Sign-on Options for Microsoft 365
        - Review Authentication Flows with AD FS (if applicable)
- **Access Management**
    - **Conditional Access**
        - Review Conditional Access
        - Review Conditional Access Policies
        - Review Azure AD Conditional Access and Federated Authentication
        - Review Zero Trust networking
        - Configure Azure AD Application Proxy (if applicable)
    - **Manage Device Access**
        - Plan for Device Compliance
        - Configure Conditional Users and Groups
        - Create Conditional Access Policies
        - Configure Conditional Access with Microsoft Endpoint Manager (Intune)
        - Review Monitoring Enrolled Devices
    - **Role Based Access Control (RBAC)**
        - Plan for Role Based Access Control
        - Review Azure RBAC roles and Azure AD administrator roles
        - Configure RBAC
        - Monitor and audit RBAC usage
    - **Solutions for External Access**
        - Plan for External Access (if applicable)
        - Manage External Access (if applicable)
        - Review Creating a Collaborative User
        - Review Customer Lockbox

Implement Microsoft 365 Threat Protection

- **Security in Microsoft 365**
    - **Review Security Solutions in Microsoft 365**

        - Review Microsoft 365 Security Center
        - Review Exchange Online Protection (EOP) with Microsoft 365 ATP
        - Review Cloud App Security
    - **Microsoft Secure Score**
        - Review Microsoft Secure Score
        - Review Secure Score Dashboard
        - Review Secure Score Analyzer
        - Review Methods for Improving Security Posture
- **Advanced Threat Protection**
    - **Exchange Online Protection**
        - Review and Configure Zero-hour Auto Purge
        - Review Phishing and Spoofing Protection
    - **Office 365 Advanced Threat Protection**
        - Review Safe Attachments
        - Review Safe Links
    - **Managing Safe Attachments**
        - Create Safe Attachment Policies
        - Create a Transport Rule to Bypass Safe Attachments
        - Review End-User Experience with Safe Attachments
        - Ensure Only Authorized Attachment Types are Allowed
    - **Managing Safe Links**
        - Create Safe Links policies in the Security Console
        - Create a Transport rule to bypass Safe Links
        - Review End-User Experience with Safe Links
    - **Azure Advanced Threat Protection**
        - Review Azure ATP
        - Configure Azure ATP
        - Review Azure ATP workspace health and events
        - Monitor Azure ATP Alerts
        - Review and configure Azure ATP Reports
    - **Microsoft Defender Advanced Threat Protection**
        - Review Microsoft Defender ATP
        - Configure Microsoft Defender ATP (if applicable)
        - Review Microsoft Defender ATP alerts (if applicable)
        - Review Microsoft Defender ATP with Azure Security Center
        - Review Windows Defender Application Guard
        - Review Windows Defender Application Control
        - Review Windows Defender Exploit Guard
- **Threat Intelligence**
    - **Using the Security Dashboard**
        - Review Threat Detection
        - Review Security Alerts
    - **Microsoft 365 Threat Investigation and Response**
        - Review Microsoft Graph
        - Review Security Dashboard
        - Review Threat Explorer

        - Review Threat Trackers
        - Review Attack Simulator
        - Review automated investigation and response in Office 365
        - Review Azure Sentinel
    - **Configure Advanced Threat Analytics**
        - Review Advanced Threat Analytics
        - Configure Advanced Threat Analytics
        - Review Managing Advanced Threat Analytics Services
- **Mobile Device Management**
    - **Plan for Mobile Application Management**
        - Plan for MAM using Enterprise Mobility + Security / Microsoft Endpoint Manager (Intune)
    - **Plan Mobile Device Management**
        - Plan for MDM using Microsoft Enterprise Mobility + Security / Microsoft Endpoint Manager (Intune)
        - Plan Policy Settings for Mobile Devices
            - Require advanced security configurations
            - Require password/PIN code of at least 6 characters with complexity
            - Prohibit mobile device password reuse
            - Set mobile device passwords to never expire
            - Prevent access from jailbroken/rooted devices
            - Lock device after period of inactivity
            - Require Encryption
            - Require antivirus and firewall be enabled
            - Require MDM policies for email profiles
        - Plan for Controlling Email and Document Access
    - **Deploy Mobile Device Management**
        - Activate Mobile Device Management Services
        - Deploy Mobile Device Management
        - Configure Domains for MDM
        - Configure an APNs Certificate for iOS devices
        - Manage Device Security Policies
        - Define Corporate Device Enrollment Policy
    - **Enrolling Devices to Mobile Device Management**
        - Enroll Windows 10 devices
        - Enroll Android devices
        - Enroll iOS devices
        - Configure Enrollment Rules
        - Ensure Users Enroll their Devices
        - Configure a Device Enrollment Manager Role
        - Review Multifactor Authentication Considerations

Implement Microsoft 365 Information Protection

- **Information Protection**
    - **Azure Information Protection (AIP)**

        - Plan for Azure Information Protection
        - Review Working with AIP Labels
        - Configure AIP Policies
        - Deploy AIP Clients
    - **Advanced Information Protection**
        - Configure RMS Templates and Labels
        - Configure Automated Labeling
        - Configure a Super User
        - Implement the AIP Tenant key
        - Implement Bulk Classification
        - Plan to Deploy the On-Premises RMS Connector (if applicable)
    - **Windows Information Protection**
        - Plan for WIP
        - Implement WIP
        - Review Working with WIP in Windows Desktop
- **Message Protection**
    - **Information Rights Management**
        - Review Microsoft 365 Encryption Options
        - Review Applying IRM Protection to Email
        - Review Rights Management in Exchange
        - Review Rights Management in SharePoint
        - Review Applying IRM Protection to SharePoint
        - Review Comparison between IRM and AIP
    - **Secure Multipurpose Internet Mail Extension**
        - Review S-MIME Digital Signatures
        - Review Applying and Verifying Digital Signatures
        - Review Encrypting and Decrypting E-mail Messages
        - Review Digital Signatures and Encryption working together
    - **Office 365 Message Encryption**
        - Review Office 365 Message Encryption
        - Review How Office 365 Message Encryption works
- **Data Loss Prevention**
    - **Data Loss Prevention**
        - Review Microsoft 365 data loss prevention
        - Review Sensitive Information Types
        - Review DLP Policies
        - Review Conditions and Actions
        - Review DLP Email Notifications
        - Review DLP Policy Tips
        - Review Policy Templates
        - Review Monitoring and analyzing sensitive data
    - **Data Loss Prevention Policies**
        - Review Choosing a Built-in Policy Template
        - Determine Choosing Locations to Protect
        - Configure DLP Rules
        - Enable the DLP Policy

- **Custom DLP Policies**
  - Review Editing a Rule
  - Review Customizing Conditions and Actions
  - Review Customizing User Notifications
  - Review Customizing User Overrides
  - Review Sending Incident Reports
- **Creating a DLP Policy to Protect Documents**
  - Review Document Protection through DLP Policies
  - Review Creating a DLP Policy
- **Policy Tips**
  - Working with Policy Tips in Email
  - Working with Policy Tips in SharePoint and OneDrive
  - Working with Policy Tips in Office 2016

- **Microsoft Cloud Application Security (MCAS)**
  - **Cloud Application Security**
    - Review Cloud App Security
    - Deploy Cloud App Security (if applicable)
    - Review Controlling your Cloud Apps with Policies
    - Review Cloud Discovery
    - Review App Connectors
    - Review Troubleshooting Microsoft Cloud App Security
  - **Using Cloud Application Security Information**
    - Review Working with discovered apps
    - Review Working with the risk score
    - Manage Alerts

Implement Microsoft 365 Compliance

- **Archiving and Retention**
  - **Archiving in Microsoft 365**
    - Review Data Governance in Microsoft 365
    - Review In-place Archiving and Records Management
    - Review In-place Archiving in Exchange
    - Review In-place Records Management in SharePoint
  - **Retention in Microsoft 365**
    - Review Retention Policies
    - Review Messaging Records Management in Exchange
    - Review Retention Tags in Exchange
  - **Retention policies in the Compliance Center**
    - Review How a Retention Policy works
    - Create a Retention Policies
    - Review Managing a Retention Policy
    - Review Event-driven Retention
  - **Archiving and Retention in Exchange**
    - Review Enabling and Disabling in-place Archiving
    - Create Retention Tags
    - Create a Retention Policy

        - Assign Retention Policies to Mailboxes
        - Review Exporting and Importing Retention Tags in a hybrid Deployment
    - **In-place records management in SharePoint**
        - Review SharePoint Records Management
        - Create a file plan to manage records
        - Plan to convert active documents to records
        - Configure in-place Records Management
- **Data Governance in Microsoft 365**
    - **Plan Compliance Needs**
        - Review Assessments in Compliance Manager
        - Configure Compliance Manager Permissions
        - Review Labels for personal data in Office 365
    - **Building ethical walls in Exchange Online**
        - Review Ethical Walls in Exchange Online
        - Create an Ethical Wall Using Distribution Groups
        - Review Best Practices for Building Ethical Walls
    - **Manage Retention in Email**
        - Configure and Apply Retention Tags
        - Assign Retention Policies to E-mail Folders
        - Add Optional Retention Policies
        - Review Removing a Retention Policy
    - **Troubleshooting Data Governance**
        - Review How Retention Age is Calculated
        - Review Troubleshooting Retention Policies that Don't Run
        - Review Troubleshooting Retention Policy Tips that Fail
        - Review Troubleshooting Sensitive Data by Validating Rules
        - Review Troubleshooting Sensitive Data by Reviewing Message Tracking Logs
- **Search and Investigations**
    - **Content Search**
        - Review Content Search
        - Design Content Search
        - Configure Search Permissions Filtering
        - Review Searching for third-party data
        - Review Public Records Act search requests
    - **Audit Log Investigations**
        - Review Audit Log Search
        - Configure Audit Policies
        - Review Viewing and Retaining the Search Results
        - Review Filtering Search Results
        - Review Exporting Search Results
        - Enable Unified Audit Logging
    - **Advanced eDiscovery**
        - Review Advanced eDiscovery
        - Create cases for Advanced eDiscovery
        - Review Searching and preparing data for Advanced eDiscovery
        - Review Analyzing data in Advanced eDiscovery

        - Review Viewing the Advanced eDiscovery Event Log
        - Review Using Express Analysis
        - Review Using Advanced Utilities

- **Microsoft Office 365 training plan and materials for OCERS team members**
    - **Develop executive introduction to essential Microsoft 365 elements**
    - **Develop training plan and materials for onboarding current OCERS team members to Microsoft 365**
    - **Develop user guides for key primary Microsoft 365 task**
    - **Microsoft 365 Administration and Security training**

Exhibit C: Minimum/Preferred Qualifications Criteria

All firms submitting a proposal in response to this RFP are required to sign and return this attachment, along with written evidence of how the respondent meets each qualification.

The undersigned hereby certifies that it fulfills the minimum/preferred qualifications outlined below, as well as the requirements contained in the RFP.

Minimum/Preferred Qualifications include:

1. Firm with 7+ years' experience performing Microsoft 365 / Office 365 migrations
2. Microsoft Certified Gold or Silver Partner Firm
3. Personnel with current Microsoft certifications for Microsoft 365 / Office 365 that will actively work on this engagement.

The undersigned hereby certifies that they are an individual authorized to bind the Firm contractually, and said signature authorizes verification of this information.

_____ _____

Authorized Signature Date

_____

Name and Title (please print)

_____

Name of Firm

Exhibit D: Proposal Cover Page and Checklist

(TO BE SUBMITTED ON FIRM'S LETTERHEAD)

Respondent Name:

Respondent Address:

By submitting this response, the undersigned hereby affirms and represents that they have reviewed the proposal requirements and have submitted a complete and accurate response to the best of their knowledge. By signing below, I hereby affirm that the respondent has reviewed the entire RFP and intends to comply with all requirements.

Respondent specifically acknowledges the following:

1. Respondent possesses the required technical expertise and has sufficient capacity to provide the services outlined in the RFP.

2. Respondent has no unresolved questions regarding the RFP and believes that there are no ambiguities in the scope of services.

3. The fee schedule submitted in response to the RFP is for the entire scope of services and no extra charges or expenses will be paid by OCERS.

4. Respondent has completely disclosed to OCERS all facts bearing upon any possible interests, direct or indirect, that Respondent believes any member of OCERS, or other officer, agent, or employee of OCERS presently has, or will have, in this contract, or in the performance thereof, or in any portion of the profits thereunder.

5. Materials contained in the proposal and all correspondence and written questions submitted during the RFP process are subject to disclosure pursuant to the California Public Records Act.

6. Respondent is not currently under investigation by any state of federal regulatory agency for any reason.

7. Except as specifically noted in the proposal, respondent agrees to all of the terms and conditions included in OCERS Services Agreement.

8. The signatory below is authorized to bind the respondent contractually.

OCERS – Technical Specifications for RFP Template

Solution Description and Pricing

1. Please provide a general description of your proposed solution based on OCERS requirements for the application as stated above.

2. For cloud and on premise, please provide a breakdown of the pricing for the proposed solution(s). Specifically for on premise, please differentiate between hardware, software licensing, subscription, professional service, support and maintenance costs.

Please indicate if third party applications and/or services are required for the solution to function correctly, as well as who is responsible for purchasing and maintaining the associated licenses or subscriptions

Product History, Roadmap and Updates

3. Please describe the history of the proposed application offering(s), including initial release date, current version number and brief development history. Not sure the applicability again here, you should be more interested in the frequency and time intervals between versions from a stability point of view [ME] This was from Gartner research "RFP Template for Cloud Financial Planning and Analysis Applications" – May 2019 – Section B: Technical Requirements – "Vendors should describe the history of their application offerings, including initial release date, current version number and development history (that is, if the offerings were developed as a marketable package or as a solution for a particular organization)."

4. Please provide information on the product development roadmaps for the proposed solution.

5. Please describe the process of new version releases, release cadence or timing, and the application of software updates to the application(s).

6. Please describe the quality assurance/testing processes to follow to determine whether a new cloud version, or an upgrade or custom modification, is suitable for release.

7. Please describe the process by which opportunities for system enhancements are identified, screened, programmed, field tested and released to customers.

8. Please describe the upgrade methodology includes a tracking system not only to report on the status of the upgrade, but also to record problems and bugs.

Product Support and Service Warranty

9. Please describe the support offerings available for proposed solution and the associated costs.

10. Please provide copies and descriptions of all warranties associated with the proposed solution and related applications.

Training, Skillset and Customer Success

11. Please describe the training and associated pricing of training that would be required/recommended for OCERS staff to complete to effectively implement and use the proposed solution. Please include required/recommended training for administrators, power users, and standard users.

12. Please describe the skills and typical job positions OCERS will need to implement, support, and use the proposed solution.

13. Please describe the extent and scope of post sales services available for supporting usage and adoption of the proposed solution.

Security Frameworks, Controls and Regulations

What control and compliance frameworks does your company adhere to (ISO, NIST, COBIT, CSA, HITRUST, etc.)?

What data security regulations does your company adhere to (PCI-DSS, HIPAA, GDPR, CCPA, GLBA, FISMA, etc.)?

System Availability

1. How do you calculate the average monthly uptime / availability rate of your solution?

2. Do you distinguish between the systems being “up” vs. being “available”?

3. What is the average monthly uptime / availability rate for the proposed solution for the past 12 months?

4. Please describe the resiliency and availability capabilities of the proposed solution. Please note any single points of failure.

5. In the past two years, how many service outages has the proposed solution experienced, and what was the longest period of downtime?

6. Please describe the proposed solutions maintenance schedule and how that may impact availability.

7. How long in advance are customers notified of scheduled maintenance windows and the subsequent estimated downtime?

OCERS – Technical Specifications for RFP Template

Service Level Agreements

8. Please provide details of your service-level agreements (SLAs), including system availability, system response times, and support ticket resolution times.

9. Please outline the available service levels, the contractually defined response and resolution times for each service level, and the associated costs.

10. What are the penalties for nonperformance according to your SLAs?

11. Are there any penalties for delayed or degraded performance?
12. Do you provide an uptime / availability guarantee?

13. Describe the protections available for customers against loss of data or data integrity issues?

14. Do you automatically notify customers of an SLA miss?

15. What is the notification window for a customer to submit a SLA claim miss? See above

16. Please provide the documented procedure for escalation if SLAs are not met.

Service and Support

17. Please provide details on the available professional services implementation and deployment offerings with associated costs.

18. Please provide details on the available post-implementation support offerings and associated costs.

19. What methods are available for getting in touch with technical support?

20. Do you offer a dashboard that shows service health?

21. Do you provide system usage and tracking tools?

22. Will we be assigned a dedicated support manager and account representative?

23. Do you have documented change management procedures?

24. Do you have documented incident prioritization procedures?

25. Describe available migration support to and from your services?

26. What support do you provide for third-party application integrations?

27. What is the process for making feature / enhancement suggestions?

28. Do you have a customer advisory panel?

Security Assessments

29. Please provide a copy of your most recent SOC 2 Type 2 report.

30. How often is your organization assessed by an independent third party and a SOC 2 Type 2 report generated?

31. Besides SOC 2 assessments, what other assessments, audits, or penetration tests are performed on your systems? Please state the frequency for each.

32. Do you provide your customer's (or their designee's) with the right to audit your systems? If so, how many audits are permitted within a 12 month period?

Personnel Management

33. What is the name of your company's Chief Information Security Officer or security lead?

34. Does your company have a dedicated Information Security department?

35. Do you outsource any of your Information Technology or Information Security functions? If so, what is outsourced?

36. Do you conduct background checks on employees, contractors and consultants?

37. Do you conduct annual mandatory security awareness training for all users of your systems?

38. How do you assess your employee's understanding of your security policies?

Risk Management

39. Does your company have a formal risk management program in place? If so, please describe.

40. Do you have cybersecurity insurance? If so, for how much? Additionally, are customers a beneficiary of this insurance too in the event of an insurance reimbursable breach?

OCERS – Technical Specifications for RFP Template

Vendor / Third Party Risk Management

41. Please describe the reliance you have on other third party suppliers to properly deliver the proposed solution.

42. Please describe the controls you have in place to ensure the failure of a third party to perform their duties does not impact your ability to deliver the proposed solution.

Data Security and Privacy

43. Describe the measures your organization takes to ensure data security to protect customer information.

44. What data encryption and security protocols are used to enable clients to protect their data?

45. Please describe the process, noting your security protocols, for how data is uploaded and transferred from your clients to you, and how it is eventually stored in a protected format on your system(s).

46. For primary (production), secondary (test), and tertiary (backup) copies of the data, in which cities, states, and countries is the data stored?

47. What controls are in place to keep client data segregated if the proposed solution is a multitenant environment?

48. Will any personnel from your company have the ability to access our data? If so, please list which job roles and how many individuals may have access to our data.

    What protocols and security measures are in place so that only authorized individuals from your company have access to our data, and how you prevent authorized individuals from unauthorized access to our data?

49. Does the proposed solution have data loss prevention (DLP) capabilities that can be configured by the customer?

50. What are the defined retention periods for customer data? Can the retention periods be configured by the customer?

51. Please describe the tools and processes for archiving historical data from the solution.

52. Please describe the tools and processes for data destruction and secure deletion when data is purged from the solution. Is a certificate of destruction provided?

53. How are data access requests from law enforcement handled?

54. Does all ownership rights to data, inputs and outputs remain with the customer for the proposed solution?

Security Incident and Response

Please provide a copy of your incident response policy/plan.

55. Please provide a copy of your breach disclosure policy.

56. Please describe the systems and processes you have in place to detect security incidents.

57. Is security monitoring performed by in-house personnel, third party personnel, or a mixture of both?

58. What criteria do you use to determine whether your customers should be notified of a security incident?

59. How and when are customers notified of security incidents?

60. Please describe how you conduct security incident investigations, capturing of evidence, and the forensic collection process.

Vulnerability Management

1. Please identify the methods, processes, and frequency associated with identifying vulnerabilities within your corporate networks and within the proposed solution.

61. When security vulnerabilities are identified in the proposed solution, please indicate the process and expected timelines to remediate the vulnerabilities.

2. Please explain who is expected to pay (customer or vendor) for vulnerability scanning / penetration testing of the proposed solution, as well as who is expected to pay for remediation of any vulnerabilities identified.

Business Continuity

OCERS – Technical Specifications for RFP Template

3. Do you have a business continuity / disaster recovery plan for the products and services we would receive from you? If so, how often is it reviewed, updated, and tested?

4. Does your Business Continuity Disaster Recovery plan address loss of technology, loss of resources, loss of facilities, and loss of suppliers?

62. Please provide a documented copy of your business continuity / disaster recovery plans, including target periods for recovery point objective (RPO) and recovery time objective (RTO).

5. In the past 12 months, have you conducted an employee Business Continuity / Disaster Recovery training exercise of the systems needed to provide your product and/or services? If so, can you share the results and areas for improvement?

6. How do you communicate to your clients during a disruption of service?

7. Do you evaluate your suppliers' preparedness as part of your business continuity or risk management functions?

8. What reliance do you have on third parties for the proper execution of recovery when there is a disruption in service?

9. If your service is limited due to a disruption, how will clients be prioritized for service restoration?

10. Is your organization able to operate effectively when key locations are closed?

63. Please describe your backup policy and strategy.

11. How is data replicated, are online and offline backups maintained, how many copies of the data are created, where are backup data sources stored, in what format is backup data stored, and how is backup data recovered?

Vendor Contacts and Communications

14. Please identify the process and the contact(s) for resolving all of the following issues:
    - Contract/SLA issues
    - Technical support issues
    - Degraded quality of service and outage issues
    - Feature enhancement requests
    - Billing/accounting issues

Termination of Service

15. If a client's contract with you expires or if a client terminates their contract with you, is their data destroyed or returned to the client?

16. If data is returned to the client, please describe the process and tools used to retrieve the data, as well as the format of the data when it is returned.

17. What provisions exist if your business terminates, is purchased or merges with another company during the term of the contract?

Architecture and Infrastructure

18. Please describe the overall architecture of the proposed solution.

19. Please how the solution will be delivered (cloud, on-premises, hosted or hybrid).

20. If it is a cloud solution, please describe the solution model. For example, the type of cloud (public, private or hybrid, single or multitenant database, etc.).

21. Please identify the number, locations, and ownership of data centers from which the solution is hosted/managed. If third-party public cloud infrastructure as a service (IaaS) providers are used, please name the vendors and describe the nature of the relationship.

22. Are systems that comprise the proposed solution solely managed by your company, solely by a third party, or by a combination of the two?

23. Does your infrastructure (including backup and disaster recovery) reside solely in the United States? Do you have components of the proposed solution that reside outside the United States?

24. How do users access the system (web browser, client application, other)? If accessed through a web browser, is there a preferred browser to use?

25. How many concurrent users can the proposed solution support?

Network

26. What is your approach to network capacity planning for the proposed solution?

27. Please describe your support for integration with cloud security gateway and/or cloud access security broker technologies.

28. Do you support the ability to connect our network directly to your network to bypass the internet?

29. Do you utilize a content delivery network (CDN) as part of the proposed solution?

30. Do you have distributed denial of service (DDoS) prevention capabilities?

31. Is all data in transit encrypted (TLS 1.2 or greater)?

32. Do you support geo-fencing to allow access to the proposed solution only from certain countries?

Storage

33. Please describe encryption options for protecting data at rest.

34. Please identify the available options for encryption key management.

35. Are there any storage limits for the proposed solution?

36. If there are storage limits, is it possible to surpass the storage limits, and are there any additional costs?

37. What data archiving options are available to the customer?

38. Do you provide e-discovery capabilities so we can search and extract relevant data as necessary?

Integration

39. Please describe the API(s) associated with the proposed solution.

40. Please identify if the API(s) can be used by the customer for data access, business functions, operational functions, user management and data import/export.

41. Do you offer an API developer portal?

42. Does the proposed solution provide native application connectors to common desktop applications?

Identity & Access Management

43. Please describe authentication controls and levels of security associated with the proposed solution.

44. Please describe how usernames and passwords are managed in the system.

45. Does the system natively support two-factor or multi-factor authentication?

46. Does the proposed solution support federation with external Single Sign-On (SSO) systems using SAML and/or OpenID?

47. Does the proposed solution support batch import / bulk upload of user accounts?

48. Does the proposed solution support directory synchronization with on premise systems such as Active Directory?

User Permissions and Roles

49. Does the system support users with different user profiles depending on their functions? Explain how your system supports each of these user profiles.

50. How many unique roles are included in the default configuration? What permissions does each role have within the system?

51. Does the proposed solution support the creation of custom roles and permissions? If so, are those configured by the vendor or the customer?

Auditing and Logging

52. Please describe the logging level / audit trail associated with user activity in the proposed solution.

53. Please describe any syslog type functionality for customers to send logs continuously to external sources (e.g. monitoring system, SIEM, etc.).

54. Can the logs be exported, and if so, in what format?