

Minnesota State Retirement System (MSRS)



REQUEST FOR PROPOSAL

RFP 85 Microsoft Dynamics GP Replacement

Date Posted: September 21, 2026

- Responses must be received not later than 3:00 PM, Central Time, October 13, 2026
- Late responses will not be considered
- As of July 1, 2025, certain terms are unenforceable in state contracts. See Session Laws, 2025 Regular Session, [Chapter 39](#), Article 2, Sec. 45.

Minnesota's Commitment to Diversity and Inclusion

The State of Minnesota is committed to diversity and inclusion in its public procurement process. The goal is to ensure that those providing goods and services to the State are representative of our Minnesota communities and include businesses owned by minorities, women, veterans, and those with substantial physical disabilities. Creating broader opportunities for historically under-represented groups provides for additional options and greater competition in the marketplace, creates stronger relationships and engagement within our communities, and fosters economic development and equality.

To further this commitment, the Department of Administration operates a program for Minnesota-based small businesses owned by minorities, women, veterans, and those with substantial physical disabilities. For additional information on this program, or to determine eligibility, please call 651.201.2402 or go to the Office of Equity in Procurement home page, at <https://mn.gov/admin/business/vendor-info/oep/>.

SPECIAL NOTICE: This is a request for proposal. It does not obligate the State of Minnesota to award a contract or complete the proposed program, and the State reserves the right to cancel this solicitation if it is considered in its best interest.

TABLE OF CONTENTS

Solicitation Content

SECTION 1 – INSTRUCTIONS TO RESPONDERS	3
SECTION 2 – SUMMARY OF SCOPE.....	4
SECTION 3 – PROPOSAL INSTRUCTIONS AND ADDITIONAL INFORMATION.....	9
SECTION 4 – PROPOSAL CONTENT	10
SECTION 5 – EVALUATION PROCEDURE AND CRITERIA	13
SECTION 6 – UNENFORCEABLE TERMS AND SOLICITATION TERMS.....	15

Solicitation Attachments

- Attachment A: Responder Declarations
- Attachment B: Exceptions to State's Terms and Conditions
- Attachment C: Cost Detail
- Attachment D: Responder Form
 - Workforce and Equal Pay Declaration Page
- Attachment E: Vendor – Technical and Security Questionnaire

Sample Contract

- Exhibit A: Contract Terms
- Exhibit B: Insurance Requirements
- Exhibit C: Specifications, Duties, and Scope of Work
- Exhibit D: Pricing

SECTION 1 – INSTRUCTIONS TO RESPONDERS

Steps for Completing Your Response	Follow the steps below to complete your response to this Solicitation: Step 1: Read the solicitation documents and ask questions, if any Step 2: Write your response Step 3: Submit your response
Incomplete Submittals	A response must be submitted along with any required additional documents. Incomplete responses that materially deviate from the required format and content may be rejected.

STEP 1 – READ THE SOLICITATION DOCUMENT & ASK QUESTIONS, IF ANY

How to Ask Questions	The contact person for questions is: Kris Wenner, kris.wenner@mnretire.gov Questions should be emailed to the contact by 3:00 PM October 1, 2026. Other personnel are not authorized to answer questions regarding this Solicitation.
----------------------	---

STEP 2 – WRITE YOUR RESPONSE

The Response Content section is in this link to [Section 4](#). Prepare a written response and supply all requested content. Responses should address the requested information and documents detailed in Section 4. **DO NOT INCLUDE** Non-Public/Trade Secret data (as defined in this link to [Minn. Stat. § 13.37](#)). **Review, sign, and include the Responder Declarations with your response.**

STEP 3 –SUBMIT YOUR RESPONSE

Where to Send Your Response	Email your response instructions. Send Proposal, Cost Detail and Additional Tasks or Activities Cost <i>as separate attached documents to one</i> email submission to kris.wenner@mnretire.gov Subject Line of Email to read “RFP 85; <i>Responder’s Company name</i>” The separate attached documents to the email should be named as follows: RFP 85 Proposal; Workday software <i>Responder’s Company name</i> RFP 85 Proposal; NetSuite software <i>Responder’s Company name</i> RFP 85 Cost Detail Workday software implementation; <i>Responder’s Company name</i> RFP 85 Cost Detail NetSuite software implementation; <i>Responder’s Company name</i> RFP 85 <i>Additional Tasks or Activities Cost</i>; <i>Responder’s Company name</i> <i>RFP 85 Third Party Software Cost</i>; <i>Responder’s Company name</i> Proposals must be received not later than 3:00 PM, CDT, October 13, 2026. Late responses will not be considered. By submitting a response, responder is making a binding legal offer for the period of time set forth below in Section 6, Conditions of Offer. By submitting a response, responder is making a binding legal offer for the period of time set forth below in Section 6, Conditions of Offer.
-----------------------------	--

SECTION 2 – SUMMARY OF SCOPE

1. Procurement Overview and Goals.

Minnesota State Retirement System (MSRS) and the State of Minnesota (State) request proposals from qualified firms that meet the minimum implementation requirements in Section 2 below for Enterprise Resource Planning (ERP) replacement of Microsoft Dynamics GP. MSRS is considering two software products for this replacement: NetSuite and Workday.

Both NetSuite and Workday are ERP systems. ERP is a type of software that organizations use to manage day-to-day business activities like accounting, procurement, project management, risk management and compliance, and supply chain operations.

The goal of this project is to select an implementation Contractor to assess our current workflows and deploy a scalable, future-proof ERP solution to replace Microsoft Dynamics GP. This will include integrations with both the State of Minnesota's Statewide Integrated Financial Tools (SWIFT), an Oracle PeopleSoft application, and with an internally created Pension Administration system, which is a Java application.

MSRS expects the Responders to include a clear project plan that outlines the scope, methodology, and timeline of the proposed solution.

2. ERP Implementation Must Have and Preferred Requirements

Once complete, the installation of the ERP system will have the following functionality and integrations:

System testing, training, and security Must Haves

1. ERP must have a sandbox or test environment.
2. In person and/or remote initial training must be provided.
3. System must be FedRAMP compliant, or Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2 or above certified.
4. If Software as a Service (SaaS), all data must be held within the US.
5. There must be a formal support channel with responses within 24 hours.
6. System must allow for integrations with various systems, with data outgoing and incoming.
7. System must support various customizable access roles.
8. Security should be mapped and easily understandable.

System testing, training, and security Preferreds

1. A training library for all types of users as well as admin should be available.
2. System preferably integrates with SSO/SAML.

General System Must Haves

1. Document attachments – pdfs, Word documents, Excel spreadsheets – must be available throughout the system.
2. Transactions are identified by user id /name, approver id/name and date and time entered, and can be retrieved through an audit trail report.
3. System provides electronic workflow process for approval of all transactions, if MSRS chooses to use the option.
4. System should allow for multiple dimensions, with parent-child relationships.

General Ledger Must Haves

1. Detailed information about each general ledger account is maintained, including description, account number, type of account, closing account, and balance.
2. System allows for up to 256 characters of general ledger transaction explanation.
3. System provides a user-controlled year-end closing process, which closes the fiscal year revenue and expense accounts to the net position account.
4. Only balanced general ledger transactions will post (debits = credits) and an error will immediately present after an attempt to post an unbalanced transaction. (Unbalanced transactions may only be posted as a "fix" with high level access intervention).
5. An audit trail is available for all journal transactions, including date and user id/name of the person entering the transaction, approving the transaction, and posting the transaction.
6. System provides the ability to add new accounts, mark accounts inactive, and merge two accounts and their related activity.
7. System provides an electronic workflow process for approval of all manual general ledger transactions.
8. System allows for up to a 10-character general ledger number.
9. System provides the ability to enter recurring and reversing general ledger entries, copy transactions, and upload transactions from Excel.
10. System provides the ability to copy general ledger accounts and funds.
11. System provides the ability to convert historic general ledger transaction information from Microsoft Dynamics GP. Data to be converted will be the current fiscal year activity plus five years, and will include transaction date, debit and credit general ledger accounts and dollar values, and transaction description.

Reporting Must Haves

1. Standard reports will be developed which can be run for specified date ranges. Reports include:
 - a. General ledger transaction list
 - b. General ledger chart of account detail
 - c. Trial balance
 - d. Statement of Fiduciary Net Position
 - e. Statement of Changes in Fiduciary Net Position
 - f. Schedule of Administrative Expenses
 - g. Budget versus expenditure report
 - h. Open purchase order encumbrance
 - i. Accounts receivable and accounts payable aging reports
 - j. Access Control report
2. Standards reports, once created, can be locked so only input parameters can be changed.
3. Standard reports can be accessed by users through a report menu.
4. Ad hoc reports can be easily generated and modified using information from all modules of the software, including reports that include information across modules.
5. Every field in the ERP is available for use in generated reports, including audit data fields such as user id.
6. Reports can be downloaded to Microsoft Excel as necessary for more in-depth analysis.
7. Reports can be run by segments of general ledger accounts, and for specified date ranges.

Reporting Preferreds

1. Reporting access should be customizable based on user.
2. Reporting dashboards should be available, customizable by user access.

Budgeting Must Haves

1. System provides the ability to establish multiple budgets by general ledger code and/or dimension.
2. Expenditures can be tracked against budgeted amounts.
3. Budget transactions are identified by user id and/or name, and date and time entered (audit trail).
4. System provides electronic workflow process for approval of all budget transactions / transfers.

Budgeting Preferreds

1. Financial and staffing budgets can be established for individual projects or contracts.

Purchasing Must Haves

1. Vendor records will tie to vendor identification numbers from an outside system.
2. Through the vendor record, recent vendor purchases, payments, and open orders can be viewed.
3. Detailed purchase orders can be set up, then downloaded in an acceptable format to establish a purchase order in an outside system (usage required by the state).
4. A process for obtaining a response file from the interface download location will be created so MSRS can be notified of the success or failure of the interface transaction and can take appropriate action.
5. Response files from the outside system will be received and write a purchase and/or contract order to a field in the ERP purchase order.
6. Purchase orders can be coded to particular projects and/or contracts.
7. Purchase orders can identify whether or not the purchased item is a capital asset establishing a capital asset record when the item is received against the purchase order. Capital asset additions will be processed through a workflow.
8. Purchasing transactions are identified by user id /name, approver id/name and date and time entered (audit trail).
9. System provides electronic workflow process for approval of all purchase order entries.

Contracting Must Haves

1. Contracts can be set up and tied to vendor records and purchase orders.
2. Contracts track all relevant information, including purchase orders, amounts, contract and payment dates, and amendment information.
3. Reports are generated reflecting expenditures against contracts.

Miscellaneous Transactions Must Haves

1. Summary general ledger transactions for various transactions in an outside system must post to the ERP. This could include contributions from employers and employees or payments of annuities and refunds.

Vendor Expenditures Must Haves

1. Payments can be made against purchase orders established in the ERP.
2. Payment data will be downloaded from the ERP to an outside system (usage required by the state) to generate payments to vendors.

3. A process for obtaining a response file from the interface download location will be created so MSRS can be notified of the success or failure of the interface transaction and can take appropriate action.
4. Response files from the outside system will be received and write warrant numbers to the expenditure detail in the ERP.
5. Reports can be generated on an as-needed basis to report payments made to vendors that day, as well as the relevant information about that payment, including contract information.
6. System provides an aging report, so payments can be released for payment as they reach the invoice due date.
7. Expenditures can be coded to particular projects or contracts.
8. Expenditure detail will accurately handle Minnesota State and multiple local tax amounts.
9. Expenditure transactions will be identified by user id /name, approver id/name, and date and time entered.
10. Copies of invoices can be stored the system and retrievable by vendor name, invoice number, or invoice amount via a scanning solution.
11. System provides electronic workflow process for approval of all expenditure transactions.
12. Vendor credit memos can be applied to an outstanding vendor invoice.

Billing Must Haves

1. System provides ability to generate invoices, creating applicable general ledger transactions.
2. System provides ability to download select invoices to an outside system.

Billing Preferreds

1. System provides ability to electronically send invoices to customers.
2. System has the ability to manage accounts receivable collections activities.

Cash Receipts Must Haves

1. Cash receipts from outside parties can be entered manually into the ERP, applied against invoices as applicable, and downloaded to an outside system (required by the state). System allows partial payments against invoices.
2. Cash receipts from members can be entered in the MSRS internal member system, then integrated with the ERP through a web service and applied against invoices as applicable. Cash receipts will the downloaded to an outside system. System allows partial payments against invoices.
3. A process for obtaining a response file from the interface download location will be created so MSRS can be notified of the success or failure of the interface transaction and can take appropriate action.
4. Cash receipts from other state agencies are received through an outside system and uploaded to the ERP, and applied against invoices as applicable. System allows partial payments against invoices.
5. All cash receipts, regardless the source, will create a general ledger transaction.
6. Transactions are identified by user id/name, approver id/name, and date and time entered (audit trail).
7. System provides electronic workflow process for approval of cash receipts.

Capital Assets Must Haves

1. Detailed information regarding all capital assets is maintained, including description, vendor, purchase price, serial and model numbers, acquisition date, location, last physical inventory date, useful life, monthly/annual depreciation amount, retirement date, replacement parts, and a photograph.

2. System provides ability to capture information regarding intangible asset information, such as internally generated software.
3. System provides a full physical inventory process.
4. System provides multiple user defined fields for each asset.
5. System calculates depreciation, with the ability to post to the general ledger.
6. Transactions are identified by user id and/or name, and date and time entered.
7. System creates general ledger entries for the disposition of an asset.
8. System provides ability to make adjustments to assets (for example, if an item was capitalized in error).
9. Transactions creating, depreciating, or retiring assets are identified by user id/name, approver id/name, and date and time entered.
10. System provides electronic workflow process for creation or retirement of assets.

Project Management Preferred

1. Vendor will provide recommendations for using ERP functionality so that projects can be established in the software, with tracking description, duration, budget, expenditures, and other project milestones; or recommend an alternative.

Access Must Haves

1. System will integrate with Microsoft Active Directory.
2. System will provide ability to limit user access to specific modules and to selections within modules. This would preferably be done with Active Directory (AD) group membership or set attributes inside the AD account.

Monitoring / Alerting Must Haves

1. System will store all audit logs as well as forward them to the central MSRS syslog system.
2. Monitoring / alerting will integrate with MSRS's monitoring system.
3. Success Messaging from outside systems must be stored for 30 days before purge.
4. Triggers send data from external member system every 30 minutes, 24/7.

SECTION 3 – PROPOSAL INSTRUCTIONS AND ADDITIONAL INFORMATION

1. Anticipated Contract Term.

The term of this contract is anticipated to be from November 16, 2026 to December 31, 2027, with a go live by October 1, 2027 with the option to extend up to an additional in one-year increments as determined by the State.

2. Question and Answer Instructions.

All questions should be submitted no later than the date and time listed in Section 1, Instructions to Responders.

MSRS anticipates that the answers to questions will be provided by October 5, 2026 at <https://www.mnretire.gov/vendors> under Current MSRS Opportunities. Any updates, such as addendums, will also be on this website.

MSRS is not obligated to answer questions submitted after the question due date and time; however; MSRS reserves the right to answer questions received after this date if it will improve the RFP.

Only personnel listed above are authorized to discuss this solicitation with responders. Contact regarding this solicitation with any personnel not listed above could result in disqualification. This provision is not intended to prevent responders from seeking guidance from state procurement assistance programs regarding general procurement questions.

If a Responder discovers any significant ambiguity, error, conflict, discrepancy, omission, or other deficiency in the solicitation, please immediately notify the contact person detailed above in writing of such error and request modification or clarification of the document.

3. Additional Tasks or Activities.

Responders are encouraged to propose additional tasks, activities, or goods above and beyond the scope of what is requested in this solicitation if they will substantially improve the results of this procurement. Any costs associated with these additional tasks, activities, or goods should be clearly marked and separated from the Cost Detail, Attachment C, associated with the tasks, activities, or goods specifically requested under this solicitation. Because cost is a factor in the evaluation of responses to this solicitation, failure to separate costs for additional tasks, activities, or goods may result in those costs being included in a responder's cost proposal and result in a lower cost score for that proposal.

SECTION 4 – PROPOSAL CONTENT

Please submit the following information:

1. Work Plan and Approach to Implementation. Responder should provide a description of the deliverables to be provided by the Responder along with a detailed work plan that identifies the time line and major tasks to be accomplished and be used as a scheduling and managing tool, as well as the basis for invoicing. Project plan to outline the scope, methodology, and timeline of the proposed solution. This document should NOT list cost detail. If cost detail is included in this document, the State may disqualify the proposal as non-responsive. Responder should provide a statement of the objectives, goals, and tasks to show or demonstrate the Responder's view and understanding of the nature of the contract, and what makes the Responder uniquely suited for this work.
2. Qualifications and Experience. Responder should provide an outline of background and experience with examples of similar work done by the Responder and a list of personnel who will conduct the project, detailing their training, and work experience. Resumes or other information about project personnel should not, if possible, contain personal telephone numbers, home addresses, or home email addresses. If it is necessary to include personal contact information, please clearly indicate in the response that personal contact information is being provided.
3. Quality Assurance and Quality Control. Responder should provide a description of the activities and processes that ensure the quality of deliverables. Responder should also provide information on how they verify quality and identify deliverables that are sub-standard. Describe any safeguards in place to secure sensitive information, non-public, or private data.
4. Future functionalities with room to grow. Describe and demonstrate functionality available for future growth, including adding additional users, and integrating new modules without a full rewrite.
5. Accessibility. Describe your company accessibility best practices and deliverables. Include explanations of the accessibility of the software, as well as the accessibility of the output, with acceptance testing upon delivery, third-party testing, other accessibility verification, and end-user testing.

The responder should complete, in an accessible format, a VPAT® 2.5 INT Rev (April 2025) for all software, hardware, and websites (as applicable) as proposed in response to the solicitation. Vendors can use the VPAT form from the ITIC VPAT site. Vendors should complete the Section 508 and WCAG 2.1A and AA sections. The EN 301 549 section can be left blank or deleted. For systems with multiple interfaces (such as an admin and user interface), report on each interface whether in the same or separate VPATs. These documents may be scored according to the solicitation evaluation.

Responders are encouraged to reference the "Vendor VPAT Guidance" at <https://mn.gov/mnit/about-mnit/accessibility/> in the "Products" tab on the Accessible IT Procurement page for information and instructions on completing the VPATs. Respondents should also review the related guidance documents on the same site for solicitation reviewers to understand expectations. The responder is strongly encouraged to provide remarks and explanation that both support compliance and detail any deficiencies, as even if you claim "supports," unless there are remarks and explanations, you may score low.

6. Security Review. Complete and submit Attachment E: Vendor – Technical and Security Questionnaire

7. **Cost Detail.** Complete and submit Attachment C, “Cost Proposal Pricing Template,” in Microsoft Excel, which is attached to this solicitation.

Responder must separate their cost proposal into Personnel Costs and Non-Personnel Costs. Non-Personnel Costs must include the cost of any third-party software licenses for two years and any other costs recommended or required by the vendor to operate the solution for the duration of two years. Any other costs shall be included as a part of personnel hourly rates. Costs must be detailed with an explanation of the cost (Attachment C).

Personnel; composition by role

Responders shall include hourly rates for each staff person assigned to this project that will be providing assistance and management of the contract. Include in hourly rate **all** costs, including:

- Actual wages of the contractor employees
- Fringe benefit costs, including employee taxes and insurance costs.
- Any additional expenses (i.e., travel, lodging)

Team Composition

For each staff person assigned to the project, Responders shall include a role title, brief role description, and a rate per hour. For all roles, Responder shall include actual or representative resumes detailing experience, training, and skillset. For all roles considered “Leadership,” Responder shall include names of proposed personnel along with resumes.

If the Responder proposes as part of the solution to provide Third Party Software, Software licenses shall be provided for a firm fixed price for the first two years which shall be listed in as a *separate* Cost Proposal. The software licenses fees will be paid upon successful installation and acceptance of the software. The costs in the proposal shall indicate the proposed price for providing the software and services for all functional areas. The price shall include custom developed application software, third-party software and annual licenses and product upgrade fees for a period of two years.

MSRS will not pay for any additional items or services whether omitted intentionally or unintentionally from the Cost Proposal. Any part of the solution not provided separately will be assumed included in the cost. Mark-ups are not allowed on Subcontractor costs and supplies. Cost information and assumptions shall be provided only in the Cost Proposal. If software is part of the proposed solution, cost proposals will be scored by adding the total cost of personnel plus the total cost of any required third-party software licenses and other costs recommend or required to operate the solution for two years.

The Overall solution cost total amount will be used for the cost score whether or not the Responder has software licenses as part of their proposed solution.

8. License Agreements, Maintenance Agreements, or Other Terms and Conditions. Responder must provide any license agreements, maintenance agreements, or any other terms and conditions relevant to the work under a resulting contract. Review and approval by the State will be required prior to contract execution. In the event Responder fails to comply with this provision, Responder agrees that it will not seek to enforce terms and conditions of any such agreement against the State. Further, failure to provide any of the pertinent documents upon request may result in the State not agreeing to sign any additional documents, rejecting your response, or cancelling the award.

Submit all requested documentation, including, but not limited to, the following documents:

1. Attachment A: Responder Declarations
2. Attachment B: Exceptions to State's Standard Terms and Conditions
3. Attachment C: Cost Proposal
4. Attachment D: Responder Forms
 - a. Workforce and Equal Pay Declaration Page
5. Attachment E: Vendor – Technical and Security Questionnaire

DO NOT INCLUDE Non-Public/Trade Secret data (as defined by Minn. Stat. § 13.37).

SECTION 5 – EVALUATION PROCEDURE AND CRITERIA

The State will conduct an evaluation of responses to this Solicitation. The evaluations will be conducted in three phases:

- Phase 1 - Review responses for responsiveness and pass/fail requirements
- Phase 2 - Evaluate responses
- Phase 3 - Select finalist(s)

1. Phase 1 – Responsiveness and Pass/Fail Requirements

The purpose of this phase is to determine if each response complies with mandatory requirements. The State will first review each proposal for responsiveness to determine if the Responder satisfies all mandatory requirements. The State will evaluate these requirements on a pass/fail basis. Mandatory Requirements. The following will be considered on a pass/fail basis:

- Responses must be received by the due date and time specified in this RFP.
- Meet all ERP Implementation Must Have requirements in Section 2.

2. Phase 2 - Evaluate Responses

Only those responses found to have met Phase 1 criteria will be considered in Phase 2.

The factors and weighting on which responses will be evaluated are:

- | | |
|--|---|
| • Work Plan and Approach to Implementation | 350 points |
| • Qualifications and Experience | 90 points |
| • Quality Assurance & Quality Control | 90 points |
| • Future functionalities with room to grow | 35 points |
| • Accessibility | 35 points |
| • Security Review | 100 points |
| • Cost Detail | <u>300 points</u>
1000 points |
| • Preference Points (if applicable) | 120 points (in addition to 1,000 available) |

Preference points are described under Solicitation Terms and will be applied to the total score after points have been awarded.

3. Phase 3 - Select Finalist(s)

Only those responses that have been evaluated under Phase 2 shall be eligible for Phase 3.

The State will make its selection based on best value, as determined by this evaluation process. The State reserves the right to pursue negotiations on any exception taken to the State's standard terms and conditions. In the event that negotiated terms cannot be reached, the State reserves the right to terminate negotiations and begin negotiating with the next highest scoring responder or take other actions as the State deems appropriate. If the State anticipates multiple awards, the State reserves the right to negotiate with more than one Responder. It is anticipated that the evaluation and selection will be completed by November 16, 2026.

SECTION 6 – UNENFORCEABLE TERMS AND SOLICITATION TERMS

Unenforceable Terms

As of July 1, 2025, certain terms are unenforceable in state contracts. See Session Laws, 2025 Regular Session, [Chapter 39](#), Article 2, Section 45.

Unenforceable terms

- (a) A contract entered into by the state shall not contain a term that:
- (1) requires the state to defend, indemnify, or hold harmless another person or entity, unless specifically authorized by statute;
 - (2) binds a party by terms and conditions that may be unilaterally changed by the other party;
 - (3) requires mandatory arbitration;
 - (4) attempts to extend arbitration obligations to disputes unrelated to the original contract;
 - (5) construes the contract in accordance with the laws of a state other than Minnesota;
 - (6) obligates state funds in subsequent fiscal years in the form of automatic renewal as defined in section 325G.56; or
 - (7) is inconsistent with chapter 13, the Minnesota Government Data Practices Act.
- (b) If a contract is entered into that contains a term prohibited in paragraph (a), that term shall be void and the contract is enforceable as if it did not contain that term.

Solicitation Terms

1. Competition in Responding

The State desires open and fair competition. Questions from responders regarding any of the requirements of the Solicitation must be submitted in writing to the Solicitation Administrator listed in the Solicitation before the due date and time. If changes are made the State will issue an addendum.

Any evidence of collusion among responders in any form designed to defeat competitive responses will be reported to the Minnesota Attorney General for investigation and appropriate action.

2. Addenda to the Solicitation

Changes to the Solicitation will be made by addendum with notification and posted in the same manner as the original Solicitation. Any addenda issued will become part of the Solicitation.

3. Data Security - Foreign Outsourcing of Work is Prohibited

All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all levels.

4. Joint Ventures

The State allows joint ventures among groups of responders when responding to the solicitation. However, one responder must submit a response on behalf of all the others in the group. The responder that submits the response will be considered legally responsible for the response (and the contract, if awarded).

5. Withdrawing Response

A responder may withdraw its response prior to the due date and time of the Solicitation. For solicitations in the SWIFT Supplier Portal, a responder may withdraw its response from the SWIFT Supplier Portal. For solicitations done any other way, a responder may withdraw its response by notifying the Solicitation Administrator in writing of the desire to withdraw.

After the due date and time of this Solicitation, a responder may withdraw a response only upon showing that an obvious error exists in the response. The showing and request for withdrawal must be made in writing to Solicitation Administrator within a reasonable time and prior to the State's detrimental reliance on the response.

6. Rights Reserved

The State reserves the right to:

- Reject any and all responses received;
- Waive or modify any informalities, irregularities, or inconsistencies in the responses received;
- Negotiate with the highest scoring Responder[s];
- Terminate negotiations and select the next response providing the best value for the State;
- Consider documented past performance resulting from a state contract may be considered in the evaluation process;
- Short list the highest scoring Responders;
- Require Responders to conduct presentations, demonstrations, or submit samples;
- Interview key personnel or references;
- Request a best and final offer from one or more Responders;
- The State reserves the right to request additional information; and
- The State reserves the right to use estimated usage or scenarios for the purpose of conducting pricing evaluations. The State reserves the right to modify scenarios, and to request or add additional scenarios for the evaluation.

7. Samples and Demonstrations

Upon request, Responders are to provide samples to the State at no charge. Except for those destroyed or mutilated in testing, the State will return samples if requested and at the Responder's expense. All costs to conduct and associated with a demonstration will be the sole responsibility of the Responder.

8. Responses are Nonpublic during Evaluation Process

All materials submitted in response to this Solicitation will become property of the State. During the evaluation process, all information concerning the responses submitted will remain private or nonpublic and will not be disclosed to anyone whose official duties do not require such knowledge. Responses are private or nonpublic data until the completion of the evaluation process as defined by Minn. Stat. § 13.591. The completion of the evaluation process is defined as the State having completed negotiating a contract with the selected responder. The State will notify all responders in writing of the evaluation results.

9. Trade Secret Information

- 9.1 Responders must not submit as part of their response trade secret material, as defined by Minn. Stat. § 13.37.
- 9.2 In the event trade secret data are submitted, Responder must defend any action seeking release of data it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments awarded against the State in favor of the party requesting the data, and any and all costs connected with that defense.
- 9.3 The State does not consider cost or prices to be trade secret material, as defined by Minn. Stat. § 13.37.
- 9.4 A responder may present and discuss trade secret information during an interview or demonstration with the State, if applicable.

10. Conditions of Offer

Unless otherwise approved in writing by the State, Responder's cost proposal and all terms offered in its response that pertain to the completion of professional and technical services and general services will remain firm for 180 days, until they are accepted or rejected by the State, or they are changed by further negotiations with the State prior to contract execution.

11. Award

Any award that may result from this solicitation will be based upon the total accumulated points as established in the solicitation. The State reserves the right to award this solicitation to a single Responder, or to multiple Responders, whichever is in the best interest of the State, providing each Responder is in compliance with all terms and conditions of the solicitation. The State reserves the right to accept all or part of an offer, to reject all offers, to cancel the solicitation, or to re-issue the solicitation, whichever is in the best interest of the State.

12. Requirements Prior to Contract Execution

Prior to contract execution, a responder receiving a contract award must comply with any submittal requests. A submittal request may include, but is not limited to, a Certificate of Insurance.

13. Targeted Group, Economically Disadvantaged Business, Veteran-Owned and Individual Preference

Unless a greater preference is applicable and allowed by law, in accordance with Minn. Stat. § 16C.16, businesses that are eligible and certified by the State as targeted group (TG) businesses, economically disadvantaged (ED) businesses, and veteran-owned businesses will receive points equal to 12% percent of the total points available as preference.

For TG/ED/VO certification and eligibility information visit the Office of Equity in Procurement website at <https://mn.gov/admin/business/vendor-info/oep/> or call the Division's Helpline at 651.201.2402.

14. Reciprocity

State shall comply with Minn. Stat. § 16C.06, subd. 7, as that applies to a non-resident vendor. This paragraph does not apply for any project in which federal funds are expended.

Solicitation Attachments

ATTACHMENT A: RESPONDER DECLARATIONS

The undersigned certifies, to the best of his or her knowledge and belief, that:

- A. **Response Contents.** The information provided is true, correct, and reliable for purposes of evaluation for potential contract award. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the Responder to suspension or debarment proceedings as well as other remedies available by law
- B. **Authorized Signature.** This Declaration is signed by the appropriate person(s), with the authority to contractually bind the Responder, as required by applicable articles, bylaws, resolutions, minutes, and ordinances.
- C. **Non-Collusion Certification.**
- The Proposal has been arrived at by the Responder independently and has been submitted without collusion and without any agreement, understanding or planned common course of action with any other vendor designed to limit fair or open competition; and
- The contents of the Response have not been communicated by the Responder or its employees or agents to any person not an employee or agent of the Responder and will not be communicated to any other individual prior to the due date and time of this Solicitation. Any evidence of collusion among Responders in any form designed to defeat competitive responses will be reported to the Minnesota Attorney General for investigation and appropriate action.
- D. **Organizational Conflicts of Interest.** To the best of Responder's knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons,
1. a vendor is unable or potentially unable to render impartial assistance or advice to the State;
 2. the vendor's objectivity in performing the contract work is or might be otherwise impaired; or
 3. the vendor has an unfair competitive advantage.
- If after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the State's Chief Procurement Officer which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organizational conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the Contractor was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to OSP, the State may terminate the contract for default. Organizational conflicts of interest terms apply to any subcontractors for this work.
- E. **Copyrighted Material Waiver.** By signing its Response, the Responder certifies that it has obtained all necessary approvals for the reproduction and distribution of the contents of its response.
- F. **Diverse Spend Reporting.** The Sample Contract contains a clause for Diverse Spend Reporting. When this clause applies, Contractor will be required to register in a free portal to report diverse spend.

Please see [Diverse Spend Reporting Frequently Asked Questions](#) for additional information.

By signing this form, Responder acknowledges and certifies compliance with all applicable requirements indicated above.

Company Name: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Phone Number: _____

Email Address: _____

ATTACHMENT B: EXCEPTIONS TO STATE'S TERMS AND CONDITIONS

The State presumes a responder agrees to the terms and conditions of this solicitation unless a responder takes specific exception to one or more of the conditions on this form.

The State reserves the right to reject, negotiate, or accept any exception listed to the State's terms and conditions (including those found in the attached Sample Contract).

INSTRUCTIONS: A responder must explicitly list all exceptions to State's terms and conditions, if any (including those found in the attached Sample Contract). Reference the clause number and page number of the State's term and condition for each of a responder's exceptions. If no exceptions exist, state "NONE" specifically on the form below. Whether or not exceptions are taken, the Responder must sign and date this form and submit it as part of their response. *(Add additional pages if necessary.)*

Clause and Page Number	Suggested Change to Clause	Explanation or Justification

By signing this form, I acknowledge that the above-named responder accepts, without qualification, all terms and conditions stated in this solicitation (including the sample contract) except those clearly outlined as exceptions above.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

ATTACHMENT C: Cost Proposal Pricing Template

See separate Microsoft Excel for the Attachment C Cost Proposal Pricing Template

ATTACHMENT D: RESPONDER FORM
Workforce and Equal Pay Declaration Page

This form is **required for all businesses** executing government contracts under the following:

Select one:

- ☐ Businesses executing a contract with **State or Metropolitan agencies** in excess of \$100,000 ([Workforce Certificate](#)) and if applicable \$500,000 ([Equal Pay Certificate](#))
- ☐ Businesses executing a contract with **University of Minnesota** for general obligation bond funded capital projects in excess of \$100,000 ([Workforce Certificate](#)) and if applicable \$500,000 ([Equal Pay Certificate](#))
- ☐ Businesses executing a contract with **Political Subdivisions** for general obligation bond funded capital projects in excess of \$250,000 ([Workforce Certificate](#)) and if applicable \$1,000,000 ([Equal Pay Certificate](#))

Select all that apply:

We are a Certificate holder:

- ☐ Workforce Certificate under the name: _____
- ☐ Equal Pay Certificate under the name: _____

We are applying/have applied for the following certificate(s):

- ☐ Workforce Certificate Application date (MM/DD/YYYY): _____
- ☐ Equal Pay Certificate Application date (MM/DD/YYYY): _____

We have not applied for one or both certificates:

- ☐ Our Company does not yet have a Workforce Certificate or Equal Pay Certificate. We acknowledge that a Workforce and, if applicable, Equal Pay Certificate, or approved exemption by MDHR is required before a contract can be executed.

We are Exempt:

- ☐ We attest to MDHR that we have not employed 40 or more employees on a single day during the prior 12 months in Minnesota or the state in where we have our primary place of business. MDHR may request the names of our employees during the previous 12 months, the date of separation, if applicable, and the current employment status and count.

Business Information

Vendor/Supplier ID	Business Name	Name of Contracting Agency
Authorized Signatory Name	Title	Date
Signature	Email	Phone

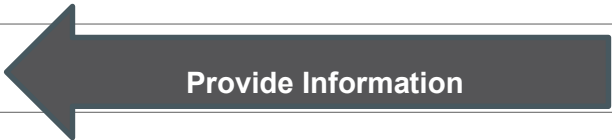
For assistance with this form, email the Minnesota Department of Human Rights Compliance.MDHR@state.mn.us



Vendor Technical and Security Questionnaire (Cloud Providers)

Version 1.3

Company Information



Name of Company: [Click here to enter text.](#)

Company Website: [Click here to enter text.](#)

Contact Person Completing the Questionnaire: [Click here to enter text.](#)

Email Address: [Click here to enter text.](#)

Phone Number: [Click here to enter text.](#)

Date of Completed Questionnaire: [Click here to enter text.](#)

Please provide a brief description of the products or services offered by your organization to MSRS: [Click here to enter text.](#)

Questionnaire Completion Instructions

1. **Respond Appropriately:** For yes or no questions, select your answer in the "Response" section. For more detailed questions, provide your response in the "Describe" column.
2. **Explain Your Answers:** In the "Describe" column, elaborate on your responses, offering additional details and explanations as necessary.
3. **Attach Supporting Documents:** Include any relevant attachments that help support and clarify your answers.



Confidential/Nonpublic: Confidential data is highly sensitive information restricted from public access and includes beneficiary data, ongoing investigation information regarding a participant, and participant information that is part of a record marked “Attorney-Client Privilege.” Medical records marked by a physician as not accessible to the patient also fall under this category. Nonpublic data pertains to internal operations and is protected from public disclosure. This includes MSRS systems documentation, internal and IT security policies, operations manuals, Continuity of Operations plans, vendor RFP responses (before a contract is awarded), draft RFPs before they are made public, draft contract documents, and documents marked “attorney-client privilege,” along with investigation data or documents.

Private Data: Private data is protected information that cannot be disclosed to the general public. This includes sensitive and personal information such as any part of a Social Security number, MSRS Account IDs, addresses, email addresses, dates of birth, personal financial information (bank account numbers, routing numbers, direct deposit details, banking institutions), medical records, disability applications and supporting documentation, driver's license numbers, passwords, challenge questions, tax withholding information, and applications for benefits.

Public Data: Public data refers to information that must be disclosed upon request by a member of the public. This includes participant information like names, gross pension amounts (once in payment status), and types of benefit (retirement, disability, survivor, refund payment). It also encompasses general organizational information such as Comprehensive Annual Financial Reports (CAFR), actuarial valuations and projections, summary data, publications, blank forms, organization charts, most MSRS policies (excluding security policies), employee handbooks, board governance manuals, position descriptions, internal audit opinions/reports, and non-protected emails.

Submission Instructions

Ensure all responses are detailed and accompanied by supporting documents where applicable.

Submit the completed questionnaire by [insert due date here].

Relationship:

Question	Document Request	Response	Describe
1.	What is your understanding of the responsibilities of your organization and our responsibilities		Click here to enter text.

Question	Document Request	Response	Describe
	during the implementation? Please provide a detailed breakdown.		
2.	What degree of control do we have over security settings and management in your solution? Describe the granular control options available.		Click here to enter text.
3.	What service model do you offer for this service? Is more than one available? Provide detailed descriptions of each service model.		Click here to enter text.
4.	What type of cloud deployment model do you offer? If the cloud is shared, how do you segregate between different clients within the cloud environment? Explain your segmentation and isolation methods.		Click here to enter text.
5.	Have you implemented this service on the cloud for other clients? How many clients, and how long was each implementation? Can you provide references? Share case studies and client references.		Click here to enter text.
6.	What is your organization's typical service-level agreements (SLAs), including uptime guarantees? Provide a detailed breakdown of SLAs.		Click here to enter text.
7.	Can you integrate with our Active Directory federated identity system using either SAML or another method to provide single sign-on (SSO) functionality from our workstations to your cloud service? Please explain the integration process in detail, including any specific requirements for SAML assertions and attributes, if applicable.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
8.	How will you support scaling of services as our needs change over time? Explain your scaling capabilities and processes.		Click here to enter text.

Question	Document Request	Response	Describe
9.	How does monitoring work in your system? What level of visibility would we have into security events and logs? Detail your monitoring and logging capabilities.		Click here to enter text.
10.	How do you manage data backup and disaster recovery? Do you test the latter process annually? Provide a detailed overview of your backup and disaster recovery processes.		Click here to enter text.
11.	What is your process for converting data from our current systems into your system, if applicable? Describe your data migration process.		Click here to enter text.
12.	Is data anonymized or scrambled in test environments? If so, how? Explain how data anonymization is performed in test environments.		Click here to enter text.
13.	What environments will be used to support the implementation? Are any of these environments deployed to the public web? Detail the environments and their configurations.		Click here to enter text.
14.	If we change vendors in the future for this service, how easy is it to retrieve and transfer all relevant data? Describe your data retrieval and transfer processes.		Click here to enter text.
15.	What third-party tools, technologies, or services do you leverage to support the solution? How are these third parties monitored? Provide details on third-party integrations and monitoring practices.		Click here to enter text.
16.	Is MSRS data ever stored, processed, or transmitted outside the continental United States, including for production or disaster recovery purposes? Additionally, is any monitoring and/or support of the system, solution, or service performed outside the continental U.S.? Please		

Question	Document Request	Response	Describe
	provide detailed information on any international locations involved in these processes.		

Security and Compliance:

Question	Document Request	Response	Describe
1.	Does your organization have a documented information security policy? If "Yes," please provide a summary.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
2.	What is your plan for notifying customers of all potential security incidents or data breaches? Do you handle incident response and mitigation? Please describe your incident response plan in detail. Additionally, have you experienced any recent breaches, and if so, how were they mitigated?		Click here to enter text.
3.	Please define your business continuity and disaster recovery processes?		Click here to enter text.
4.	How does your organization protect data confidentiality and integrity? Please define data residency.		Click here to enter text.
5.	Is your organization compliant with relevant data protection and privacy regulations (e.g., GDPR, HIPAA, CCPA, FedRamp)? If "Yes," please specify the regulations with which you are compliant.	Yes ☐ No ☐ n/a ☐	Click here to enter text.

Question	Document Request	Response	Describe
6.	Does your organization perform regular privacy impact assessments?	Yes ☐ No ☐ n/a ☐	Click here to enter text.
7.	What measures do you have in place to protect data privacy and security?		Click here to enter text.
8.	List any security certifications or standards that your organization complies with (e.g., ISO 27001, SOC 2 or FedRamp).		Click here to enter text.

Access Control and Authentication:

Question	Document Request	Response	Describe
1.	How are controls established to support appropriate and timely responses to job changes and job terminations while ensuring internal controls and security are not compromised?		Click here to enter text.
2.	Describe the screening process, including background checks for new employees and continued periodic screening for existing employees.		Click here to enter text.
3.	Please explain the process that your organization has in place to notify system administrators whenever users are terminated, ensuring the removal of their access permissions.		Click here to enter text.
4.	How does your organization handle the reporting of significant IT events or failures that may impact financial reporting, such as security breaches,		Click here to enter text.

Question	Document Request	Response	Describe
	major system failures, or regulatory failures? Are these incidents reported to senior management and customers?		

IT Management and Compliance:

Question	Inquiry	Response	Describe
1.	How does your organization define, communicate, review, and assess compliance with privacy, confidentiality, and corporate security standards within the organization?		Click here to enter text.
2.	Can you explain how your organization defines, implements, and maintains security levels for each data classification? Are these security levels periodically re-evaluated and modified based on specific criteria?		Click here to enter text.

Risk Assessment and Compliance:

Question	Inquiry	Response	Describe
1.	What procedures does your IT department use to assess information risks, and how does it identify the need for policies and procedures?		Click here to enter text.
2.	How often does your organization undergo third-party security assessments, audits, and/or		Click here to enter text.

Question	Inquiry	Response	Describe
	penetration tests? Can you provide the most recent results? Share the frequency and results of security assessments.		
3.	Please provide a copy of your SOC 2 Type II report or the most recent independent security assessment for us to review the implementation of security controls.		Click here to enter text.
4.	What processes or tools are in place to identify and mitigate vulnerabilities within your information systems?		Click here to enter text.

Documentation and Internal Controls:

Question	Inquiry	Response	Describe
1.	How does your organization handle the documentation of significant IT processes and activities? How are these documents maintained, updated, and communicated to IT staff?		Click here to enter text.
2.	How does IT management monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities and reviews?		Click here to enter text.
3.	How does IT management ensure independent internal control reviews of third-party service providers who support significant processes for financial reporting and disclosure? Do you obtain and review copies of SOC 2 Type II reports or other		Click here to enter text.

Question	Inquiry	Response	Describe
	independent audit reports from these providers?		

Change Management and Development:

Question	Inquiry	Response	Describe
1.	What change management tools does your organization use to capture and control application changes throughout the entire change cycle? For example, do you use change control software, checklists, or procedure outlines?		Click here to enter text.
2.	How does your organization handle the approval and tracking of change requests? Can you describe the process involved?		Click here to enter text.
3.	How is write access to the production environment granted to developers, and how is it monitored and periodically reviewed for security purposes?		Click here to enter text.
4.	Does the SDLC align to a secure software development standard? (e.g., Microsoft Security Development Life Cycle) If "Yes," please provide details.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
5.	Will all development be performed onshore? If "No," please provide information about offshoring or outsourcing arrangements.	Yes ☐ No ☐ n/a ☐	Click here to enter text.

Question	Inquiry	Response	Describe
6.	Is cybersecurity training provided to developers? If "Yes," please provide details about the training programs.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
7.	Will trusted information assurance controls be used to safeguard the development environment (e.g., secure network configurations, strict access controls, dynamic/static vulnerability management tools, penetration testing)?		Click here to enter text.
8.	Is open-source software validated prior to use? If "Yes," please provide details about the validation process.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
9.	Are codified software tests and configuration standards leveraged in development? If "Yes," please provide details about the testing and configuration standards.		

Security Organization and Management:

Question	Inquiry	Response	Describe
1.	How did the management create the information security program while taking into account the evaluation of risks associated with the confidentiality, integrity, and availability of information?		Click here to enter text.
2.	Could you describe how management ensures the appropriate segregation of duties among		Click here to enter text.

Question	Inquiry	Response	Describe
	personnel who are involved in the information security function?		
3.	Describe how the privacy of individual client information is protected from comingling or unapproved access.		Click here to enter text.
4.	Can you confirm if management has published a comprehensive set of policies and procedures that align with the organization's objectives regarding information confidentiality, integrity, and availability? If "Yes," please provide details on the high-level security strategy, security policies, security procedures, and technical security configurations implemented.	Yes ☐ No ☐ n/a ☐	Click here to enter text.
5.	Could you describe the formal documented security administration process in place to ensure that all application access is properly approved within your organization?		Click here to enter text.
6.	How does management conduct periodic reviews of application access permissions to ensure that access levels are appropriate and aligned with job responsibilities?		Click here to enter text.
7.	How are monitoring procedures and audit trails designed within your organization to enable management to monitor the environment for potential unauthorized activity effectively?		Click here to enter text.
8.	Could you provide information on how management conducts periodic reviews of monitoring or audit trail output to identify potential unauthorized activity? Additionally,		Click here to enter text.

Question	Inquiry	Response	Describe
	please describe the actions taken when such activity is identified.		
9.	Can you explain the formal security administration process in place to grant, change, and remove direct access to databases in a controlled manner?		Click here to enter text.
10.	How does management ensure that direct data access, specifically Database Administrator access, is periodically reviewed to ensure that access levels align with job responsibilities?		Click here to enter text.
11.	Please describe the process established within your organization to notify system administrators whenever database users are terminated, ensuring the removal of their access permissions.		Click here to enter text.
12.	Could you provide an overview of the monitoring procedures and audit trails designed to enable management to monitor the environment for potential unauthorized activity effectively?		Click here to enter text.
13.	How does management carry out periodic reviews of monitoring or audit trail output to identify potential unauthorized activity? Moreover, please explain the actions taken when such activity is identified.		Click here to enter text.
14.	Can you provide an overview of the encryption methods and technologies implemented within your organization to safeguard data both in transit and at rest?		Click here to enter text.
15.	How are encryption keys managed and protected to ensure the security of encrypted data?		Click here to enter text.
16.	What encryption standards and protocols do you adhere to when securing sensitive data, and how are these regularly updated to meet evolving security needs?		Click here to enter text.

Question	Inquiry	Response	Describe
17.	Are there specific encryption measures in place for data backups and archives, and if so, could you describe those procedures?		Click here to enter text.
18.	How do you monitor and audit the effectiveness of encryption mechanisms to ensure compliance and identify potential vulnerabilities?		Click here to enter text.
19.	In the event of a data breach or security incident, what is the procedure for assessing and mitigating the impact on encrypted data, and how is notification handled as needed?		Click here to enter text.
20.	Can you explain the formal security administration process implemented by management to grant, change, and remove access at the operating system level?		Click here to enter text.
21.	How does management conduct periodic reviews of operating system access to ensure that the security administration process is functioning correctly, and access levels align with job responsibilities?		Click here to enter text.
22.	Please confirm whether management has implemented anti-virus, anti-spyware, and SPAM software within your organization. If implemented, kindly provide details on the specific software in use.		Click here to enter text.
23.	Are there any third-party service providers that are used to manage your applications, network, or information system facilities? If so, identify whether there are any service level agreements or contracts in place with these entities. Also identify if a SOC 2 Type II report is available for each service provider.		Click here to enter text.

Question	Inquiry	Response	Describe
24.	What controls are in place to monitor noncompliance with service level agreements with third-party service providers? How is the performance of these providers monitored and assessed?		Click here to enter text.
25.	Are these third-party vendors located in the United States? If not, specify the countries and detail how international data transfers and data residency is managed.		Click here to enter text.

Additional System Considerations

1.	MSRS has a preference to be platform agnostic and use open standards. Considerations include: a. If on-premises, assess difficulty of moving to the cloud. b. If cloud, assess difficulty of moving to different vendors or bringing it on premises.		Click here to enter text.
2.	If Testing-as-a-Service (TaaS), describe the process/difficulty of moving data in and out of the ERP.		Click here to enter text.

3.	Does ERP have an Application Programming Interface (API), and does that API have open standards?		Click here to enter text.
4.	Does authentication integrate with Active Directory (AD)? There should be some options in list of priority, avoiding locally created/defined users wherever possible.		Click here to enter text.
5.	Single Sign On (SSO), also known as Central Identity Provide and computer identity credentials, from MSRS IDP (SAML preferred) Kerberos ticket passthrough (for client side) Direct lap query/connection.		Click here to enter text.
6.	Is there Lightweight Directory Access Protocol (LDAP) account sync?		Click here to enter text.
7.	Is there auto provisioning of application side users?		Click here to enter text.
8.	Authorization through role in active directory at MSRS must include security group membership integration with AD, preferably with nested group membership support.		Click here to enter text.

9.	SSO/IDP group pass. Role memberships are passed via the SSO message and then mapped to authorize on the app side.		Click here to enter text.
10.	Authorizing can be mapped to a queried/sync'd list of roles.		Click here to enter text.
11.	Logging and alerting should happen though centralized MSRS log system. Getting logs into the log system can come from a variety of methods: a. Logging to syslog b. Logging to anyplace a logstash/filebeat agent can get the logs		Click here to enter text.
12.	Avoid vendor lock-in for cloud platforms.		Click here to enter text.
13.	SaaS tools should have an easy way to get data in/out of it and should run from a w3 standards compliant browser.		Click here to enter text.
14.	Operating System a. Server side: Run on Ubuntu Linux LTS wherever possible. b. Containers: Containerized applications are becoming preferred.		Click here to enter text.

	c. Client side: Run on Windows 10 wherever possible. Linux support appreciated but not required.		
15.	Must have and provide robust documentation including but not limited to security API.		Click here to enter text.
16.	What is the maintenance schedule for upgrades/updates?		Click here to enter text.
17.	What is the integration process?		Click here to enter text.



Sample State of Minnesota Professional and Technical Services Contract

SWIFT Contract Number: _____

This Contract is between the State of Minnesota, acting through its acting through the Executive Director of the Minnesota State Retirement System, 60 Empire Drive, St. Paul, Minnesota, 55103 (“MSRS” or “State”) and Contractor Inc. whose designated business address is XXXXXXX (“Contractor”). State and Contractor may be referred to jointly as “Parties.”

Recitals

1. State issued a Request for Proposal RFP 85 Microsoft Dynamics GP Replacement (“Solicitation”);
2. Contractor provided a response to the Solicitation indicating its interest in and ability to provide the goods or services requested in the Solicitation; and
3. Subsequent to an evaluation in accordance with the terms of the Solicitation and negotiation, the Parties desire to enter into a contract.

Accordingly, the Parties agree as follows:

Contract

1. Term of Contract

- 1.1 Effective date. XXXX, or the date the State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later. The Contractor must not begin work under this Contract until this Contract is fully executed and the Contractor has been notified by the State’s Authorized Representative to begin the work.
- 1.2 Expiration date. XXXX, or until all obligations have been satisfactorily fulfilled, whichever occurs first. The contract may be extended in time increments as determined by the State, through a duly executed amendment.

2. Contractor’s Duties

The Contractor shall perform all duties described in this Contract to the satisfaction of the State.

The Contractor, who is not a State employee, shall: XXX

3. Representations and Warranties

- 3.1 Under Minn. Stat. §§ 15.061 and 16C.03, subd. 3, and other applicable law the State is empowered to engage such assistance as deemed necessary.
- 3.2 Contractor warrants that it is duly qualified and shall perform its obligations under this Contract in accordance with the commercially reasonable standards of care, skill, and diligence in Contractor's industry, trade, or profession, and in accordance with the specifications set forth in this Contract, to the satisfaction of the State.
- 3.3 Contractor warrants that it possesses the legal authority to enter into this Contract and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Contract, or any part thereof, and to bind Contractor to its terms.

4. Time

The Contractor must comply with all the time requirements described in this Contract. In the performance of this Contract, time is of the essence.

5. Consideration and Payment

5.1

Consideration. The State will pay for performance by the Contractor under this Contract as follows:

- 5.1.1 Compensation. The Contractor will be paid: XXX
- 5.1.2 Total obligation. The total obligation of the State for all compensation and reimbursements to the Contractor under this Contract will not exceed \$ XXX

5.2 Payment.

5.2.1 Invoices. The State will promptly pay the Contractor after the Contractor presents an itemized invoice for the goods received or services actually performed, and the State's Authorized Representative accepts the invoiced goods or services. Invoices must be submitted timely and according to the following schedule: XXX

5.2.1.1.1 Contractor will not submit invoices for the Contract more frequent than on a monthly basis. Summary type invoicing must include these fields:

- Purchase Order Number
- Contract Number
- Invoice Number
- MSRS Authorized Representative
- Dates and hours of service
- Description of specific task or deliverable
- Explanation of work performed per charge indicated on the invoice

To ensure prompt payment, all invoices must be sent by E-mail to:

|

msrs_ap@ mnretire.gov (In the subject line include the contract number)

Or

Minnesota State Retirement System
Accounts Payable
60 Empire Drive, Suite 300
St. Paul, Minnesota 55103-3000

- 5.2.2 Retainage. Under Minn. Stat. § 16C.08, subd. 2 (10), no more than 90 percent of the amount due under this Contract may be paid until the final product of this Contract has been reviewed by the State. The balance due will be paid when the State determines that the Contractor has satisfactorily fulfilled all the terms of this Contract.
- 5.2.3 Conditions of payment. All services delivered by the Contractor under this Contract must be performed to the State's satisfaction and in accordance with all applicable federal, state, and local laws, ordinances, rules, and regulations including business registration requirements of the Office of the Secretary of State. The Contractor will not receive payment for work found by the State to be unsatisfactory or performed in violation of federal, state, or local law.

6. Authorized Representative

- 6.1 The State's Authorized Representative is XXX or his/her/their successor or delegate, and has the responsibility to monitor the Contractor's performance.
- 6.2 Contractor's Authorized Representative. The Contractor's Authorized Representative is XXX at the following business address and telephone number: XXXX, or his/her/their successor. If the Contractor's Authorized Representative changes at any time during this Contract, the Contractor must immediately notify the State.

7. Exhibits

The following Exhibits are attached and incorporated into this Contract. In the event of a conflict between the terms of this Contract and its Exhibits, or between Exhibits, the order of precedence is first the Contract, and then in the following order:

- Exhibit A: Contract Terms
Exhibit B: Insurance Terms
Exhibit C: Specifications, Duties, and Scope of Work
Exhibit D: Price and Payment Schedule

1. State Encumbrance Verification

Individual certifies that funds have been encumbered as required by Minn. Stat. §§ 16A.15 and 16C.05

Print Name: _____

Signature: _____

Title: _____ Date: _____

SWIFT Contract No. _____

2. Contractor

The Contractor certifies that the appropriate person has executed the Contract on behalf of the Contractor as required by applicable articles, bylaws, resolutions, or ordinances.

Print Name: _____

Signature: _____

Title: _____ Date: _____

3. Minnesota State Retirement System

With delegated authority

Print Name: _____

Signature: _____

Title: _____ Date: _____

4. Commissioner of Administration

As delegated to The Office of State Procurement

Print Name: _____

Signature: _____

Title: _____ Date: _____

Admin ID: _____

Exhibit A: Contract Terms

1. Prompt Payment and Invoicing.

- 1.1 Prompt Payment. The State will pay the Contractor pursuant to Minn. Stat. § 16A.124, which requires payment within 30 days following receipt of an undisputed invoice, or merchandise or service, whichever is later. Terms requesting payment in less than 30 days will be changed to read “Net 30 days.” Notwithstanding the foregoing, the State may pay the Contractor in advance for purchases as allowed pursuant to Minn. Stat. §16A.065.

The payment for each order will only be made for goods received or services actually performed that have been accepted by the ordering entity, and meet all terms, conditions, and specifications of the Contract and the ordering document.

- 1.2 Invoicing. The invoice must be submitted as described in the Contract Consideration and Payment Section 5.2.1. See Section 5.2.1, for minimum invoice requirements

2. Assignment, Amendments, Waiver, and Contract Complete.

- 2.1 Assignment. The Contractor may neither assign nor transfer any rights or obligations under this Contract without the prior consent of the State and a fully executed assignment agreement, executed and approved by the authorized parties or their successors.
- 2.2 Amendments. Any amendment to this Contract must be in writing and will not be effective until it has been executed and approved by the authorized parties or their successors.
- 2.3 Waiver. If the State fails to enforce any provision of this Contract, that failure does not waive the provision or its right to enforce it.
- 2.4 Contract Complete. This Contract contains all negotiations and agreements between the State and the Contractor. No other understanding regarding this Contract, whether written or oral, may be used to bind either party.

3. Termination.

- 3.1 Termination for Convenience. The State or Commissioner of Administration may cancel this Contract at any time, with or without cause, upon 30 days’ written notice to the Contractor. Upon termination for convenience, the Contractor will be entitled to payment, determined on a pro rata basis, for services or goods satisfactorily performed or delivered.
- 3.2 Termination for Breach. The State may terminate this Contract, with cause, upon 30 days’ written notice to Contractor of the alleged breach and opportunity to cure. If after 30 days, the alleged breach has not been remedied, the State may immediately terminate the Contract.
- 3.3 Termination for Insufficient Funding. The State may immediately terminate this Contract if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued at a level sufficient to allow for the payment of the services addressed within this Contract. Termination must be by written notice to the Contractor. The State is not obligated to pay for any services that are provided after notice and effective date of termination. However, the Contractor will be entitled to payment, determined on a pro rata basis, for services satisfactorily performed to the extent that dedicated funds are available. The State will not be assessed any penalty if the Contract is terminated because of the decision of the Minnesota

Legislature, or other funding source, not to appropriate funds. The State must provide the Contractor notice of the lack of funding. This notice will be provided within a reasonable time of the State's receiving notice.

4. Force Majeure.

Neither party shall be responsible to the other or considered in default of its obligations within this Contract to the extent that performance of any such obligations is prevented or delayed by acts of God, war, riot, disruption of government, or other catastrophes beyond the reasonable control of the party unless the act or occurrence could have been reasonably foreseen and reasonable action could have been taken to prevent the delay or failure to perform. A party relying on this provision to excuse performance must provide the other party prompt written notice of the inability to perform and take all necessary steps to bring about performance as soon as practicable.

5. Indemnification.

- 5.1 In the performance of this Contract, the Indemnifying Party must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the State, to the extent caused by Indemnifying Party's:

- Intentional, willful, or negligent acts or omissions; or
- Actions that give rise to strict liability; or
- Breach of contract or warranty.

The Indemnifying Party is defined to include the Contractor, Contractor's reseller, any third party that has a business relationship with the Contractor, or Contractor's agents or employees, and to the fullest extent permitted by law. The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Indemnifying Party may have for the State's failure to fulfill its obligation under this Contract.

- 5.2 Nothing within this Contract, whether express or implied, shall be deemed to create an obligation on the part of the State to indemnify, defend, hold harmless or release the Indemnifying Party. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

6. Governing Law, Jurisdiction, and Venue.

Minnesota law, without regard to its choice-of-law provisions, governs this Contract. Venue for all legal proceedings out of this Contract, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

7. Foreign Outsourcing of Work Prohibited.

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by all subcontractors.

8. Subcontracting and Subcontract Payment.

- 8.1 Subcontracting Allowed. A subcontractor is a person or company that has been awarded a portion of the Contract by Contractor. Only subcontractors that have been approved by the State's Authorized Representative can be used for this Contract.

After the effective date of the Contract, the Contractor shall not, without prior written approval of the State's Authorized Representative, subcontract for the performance of any of the Contractor's obligations that were not already approved for subcontracting when the Contract was awarded. During this Contract, if an approved

subcontractor is determined to be performing unsatisfactorily by the State's Authorized Representative, the Contractor will receive written notification that the subcontractor can no longer be used for this Contract.

Contractor will require that the provisions of this Contract apply with equal force and effect to all approved subcontractors engaged by the Contractor. Notwithstanding approval by the State, no subcontract shall serve to terminate or in any way affect the primary legal responsibility of the Contractor for timely and satisfactory performances of the obligations contemplated by the Contract.

8.2 Subcontractor Payment. Contractor must pay any subcontractor in accordance with Minn. Stat. § 16A.1245.

9. Data Disclosure.

Under Minn. Stat. § 270C.65, subd. 3 and other applicable law, the Contractor consents to disclosure of its social security number, federal employer tax identification number, and Minnesota tax identification number, already provided to the State, to federal and state agencies, and state personnel involved in the payment of state obligations. These identification numbers may be used in the enforcement of federal and state laws which could result in action requiring the Contractor to file state tax returns, pay delinquent state tax liabilities, if any, or pay other state liabilities.

10. Government Data Practices.

The Contractor and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (or, if the State contracting party is part of the Judicial Branch, with the Rules of Public Access to Records of the Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by the State under this Contract, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the Contractor under this Contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. Ch. 13, by either the Contractor or the State.

If the Contractor receives a request to release the data referred to in this clause, the Contractor must immediately notify and consult with the State's Authorized Representative as to how the Contractor should respond to the request. The Contractor's response to the request shall comply with applicable law.

11. Intellectual Property Rights.

11.1 Definitions. For the purpose of this Section, the following words and phrases have the assigned definitions:

- 11.1.1 "Documents" are the originals of any databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, disks, or other materials, whether in tangible or electronic forms, prepared by the Contractor, its employees, agents, or subcontractors, in the performance of this Contract.
- 11.1.2 "Pre-Existing Intellectual Property" means intellectual property developed prior to or outside the scope of this Contract, and any derivatives of that intellectual property.
- 11.1.3 "Works" means all inventions, improvements, discoveries (whether or not patentable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by the Contractor, its employees, agents, and subcontractors, either individually or jointly with others in the performance of this Contract. "Works" includes Documents.

11.2 Ownership. The State owns all rights, title, and interest in all of the intellectual property rights, including copyrights, patents, trade secrets, trademarks, and service marks in the Works and Documents created and paid for under this Contract. The Documents shall be the exclusive property of the State and all such

Documents must be immediately returned to the State by the Contractor upon completion or cancellation of this Contract. To the extent possible, those Works eligible for copyright protection under the United States Copyright Act will be deemed to be “works made for hire.” The Contractor assigns all right, title, and interest it may have in the Works and the Documents to the State. The Contractor must, at the request of the State, execute all papers and perform all other acts necessary to transfer or record the State’s ownership interest in the Works and Documents.

11.3 Pre-existing Intellectual Property. Each Party shall retain ownership of its respective Pre-Existing Intellectual Property. The Contractor grants the State a perpetual, irrevocable, non-exclusive, royalty free license for Contractor’s Pre-Existing Intellectual Property that are incorporated in the products, materials, equipment, deliverables, or services that are purchased through the Contract.

11.4 Obligations.

11.4.1 Notification. Whenever any invention, improvement, or discovery (whether or not patentable) is made or conceived for the first time or actually or constructively reduced to practice by the Contractor, including its employees and subcontractors, in the performance of this Contract, the Contractor will immediately give the State’s Authorized Representative written notice thereof, and must promptly furnish the State’s Authorized Representative with complete information and/or disclosure thereon.

11.4.2 Representation. The Contractor must perform all acts, and take all steps necessary to ensure that all intellectual property rights in the Works and Documents are the sole property of the State, and that neither Contractor nor its employees, agents, or subcontractors retain any interest in and to the Works and Documents. The Contractor represents and warrants that the Works and Documents do not and will not infringe upon any intellectual property rights of other persons or entities.

11.4.3 Indemnification. Notwithstanding any other indemnification obligations addressed within this Contract, the Contractor will indemnify; defend, to the extent permitted by the Attorney General; and hold harmless the State, at the Contractor’s expense, from any action or claim brought against the State to the extent that it is based on a claim that all or part of the Works or Documents infringe upon the intellectual property rights of others. The Contractor will be responsible for payment of any and all such claims, demands, obligations, liabilities, costs, and damages, including but not limited to, attorney fees. If such a claim or action arises, or in the Contractor’s or the State’s opinion is likely to arise, the Contractor must, at the State’s discretion, either procure for the State the right or license to use the intellectual property rights at issue or replace or modify the allegedly infringing works or documents as necessary and appropriate to obviate the infringement claim. This remedy of the State will be in addition to and not exclusive of other remedies provided by law.

12. Copyright.

The Contractor shall save and hold harmless the State of Minnesota, its officers, agents, servants and employees, from liability of any kind or nature, arising from the use of any copyrighted or noncopyrighted compositions, secret process, patented or nonpatented invention, article or appliance furnished or used in the performance of the Contract.

13. Contractor’s Documents.

Any licensing and maintenance agreement, or any order-specific agreement or document, including any pre-installation, linked or “click through” agreement that is allowed by, referenced within or incorporated within the Contract whenever the Contract is used for a State procurement, whether directly by the Contractor or through a Contractor’s agent, subcontractor or reseller, is agreed to only to the extent the terms within any such agreement or document do not

conflict with the Contract or applicable Minnesota or Federal law, and only to the extent that the terms do not modify, diminish or derogate the terms of the Contract or create an additional financial obligation to the State. Any such agreement or document must not be construed to deprive the State of its sovereign immunity, or of any legal requirements, prohibitions, protections, exclusions or limitations of liability applicable to this Contract or afforded to the State by Minnesota law. A State employee's decision to choose "accept" or an equivalent option associated with a "click-through" agreement does not constitute the State's concurrence or acceptance of terms, if such terms are in conflict with this section.

14. State Audits.

Under Minn. Stat. § 16C.05, subd. 5, the Contractor's books, records, documents, and accounting procedures and practices relevant to this Contract are subject to examination by the State, the State Auditor, or Legislative Auditor, as appropriate, for a minimum of six years from the expiration or termination of this Contract.

15. Diverse Spend Reporting.

If the total value of the Contract may exceed \$500,000, including all extension options, Contractor must track and report, on a quarterly basis, the amount paid to diverse businesses both: 1) directly to subcontractors performing under the Contract, and 2) indirectly to diverse businesses that provide supplies/services to your company (in proportion to the revenue from this Contract compared to Contractor's overall revenue). When this applies, Contractor will register in a free portal to help report the Tier 2 diverse spend, and the requirement continues as long as the Contract is in effect.

16. Publicity and Endorsement.

16.1 Publicity. Any publicity regarding the subject matter of this Contract must identify the State as the sponsoring agency and must not be released without prior written approval from the State's Authorized Representative. For purposes of this provision, publicity includes notices, informational pamphlets, press releases, information posted on corporate or other websites, research, reports, signs, and similar public notices prepared by or for the Contractor individually or jointly with others, or any subcontractors, with respect to the program, publications, or services provided resulting from this Contract.

16.2 Endorsement. The Contractor must not claim that the State endorses its products or services.

17. Debarment by State, its Departments, Commissions, Agencies, or Political Subdivisions.

Contractor certifies that neither it nor its principals is presently debarred or suspended by the Federal government, the State, or any of the State's departments, commissions, agencies, or political subdivisions. Contractor's certification is a material representation upon which the Contract award was based. Contractor shall provide immediate written notice to the State's Authorized Representative if at any time it learns that this certification was erroneous when submitted or becomes erroneous by reason of changed circumstances.

18. Contingency Fees Prohibited.

Pursuant to Minn. Stat. § 10A.06, no person may act as or employ a lobbyist for compensation that is dependent upon the result or outcome of any legislation or administrative action.

19. Certification of Nondiscrimination (in accordance with Minn. Stat. § 16C.053).

If the value of this Contract, including all extensions, is \$50,000 or more, Contractor certifies it does not engage in and has no present plans to engage in discrimination against Israel, or against persons or entities doing business in Israel, when making decisions related to the operation of the vendor's business. For purposes of this section, "discrimination" includes but is not limited to engaging in refusals to deal, terminating business activities, or other actions that are intended to limit commercial relations with Israel, or persons or entities doing business in Israel, when such actions are taken in a manner that in any way discriminates on the basis of nationality or national origin and is not based on a valid business reason.

20. Non-discrimination (in accordance with Minn. Stat. § 181.59).

The Contractor will comply with the provisions of Minn. Stat. § 181.59.

21. E-Verify Certification (in accordance with Minn. Stat. § 16C.075).

For services valued in excess of \$50,000, Contractor certifies that as of the date of services performed on behalf of the State, Contractor and all its subcontractors will have implemented or be in the process of implementing the federal E-Verify Program for all newly hired employees in the United States who will perform work on behalf of the State.

Contractor is responsible for collecting all subcontractor certifications and may do so utilizing the [E-Verify Subcontractor Certification Form](#). All subcontractor certifications must be kept on file with Contractor and made available to the State upon request.

22. Affirmative Action Requirements

The State intends to carry out its responsibility for requiring affirmative action by its contractors.

- 22.1 Covered Contracts and Contractors. If the Contract exceeds \$100,000 and the Contractor employed 40 or more full-time employees on a single working day during the previous 12 months in Minnesota or in the state where it has its principal place of business, then the Contractor must comply with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600.
- 22.2 General. Minn. R. 5000.3400-5000.3600 implements Minn. Stat. § 363A.36. These rules include, but are not limited to, criteria for contents, approval, and implementation of affirmative action plans; procedures for issuing certificates of compliance and criteria for determining a contractor's compliance status; procedures for addressing deficiencies, sanctions, and notice and hearing; annual compliance reports; procedures for compliance review; and contract consequences for non-compliance. The specific criteria for approval or rejection of an affirmative action plan are contained in various provisions of Minn. R. 5000.3400-5000.3600 including, but not limited to, Minn. R. 5000.3420-5000.3500 and 5000.3552-5000.3559.
- 22.3 Disabled Workers. The Contractor must comply with the following affirmative action requirements for disabled workers.

AFFIRMATIVE ACTION FOR DISABLED WORKERS

- 22.3.1 The Contractor must not discriminate against any employee or applicant for employment because of physical or mental disability in regard to any position for which the employee or applicant for employment is qualified. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified disabled persons without discrimination based upon their physical or mental disability in all employment practices such as the following: employment, upgrading, demotion or transfer, recruitment, advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.
- 22.3.2 The Contractor agrees to comply with the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.
- 22.3.3 In the event of the Contractor's noncompliance with the requirements of this clause, actions for noncompliance may be taken in accordance with Minn. Stat. § 363A.36, and the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.
- 22.3.4 The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices in a form to be prescribed by the Commissioner. Such notices must state the Contractor's obligation under the law to take affirmative action to employ and advance in

employment qualified disabled employees and applicants for employment, and the rights of applicants and employees.

22.3.5 The Contractor must notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of Minn. Stat. § 363A.36, of the Minnesota Human Rights Act and is committed to take affirmative action to employ and advance in employment physically and mentally disabled persons.

22.4 Consequences. The consequences for the Contractor's failure to implement its affirmative action plan or make a good faith effort to do so include, but are not limited to, suspension or revocation of a certificate of compliance by the Commissioner, refusal by the Commissioner to approve subsequent plans, and termination of all or part of this Contract by the Commissioner or the State.

22.5 Certification. The Contractor hereby certifies that it is in compliance with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600 and is aware of the consequences for noncompliance.

23. Equal Pay Certification.

If required by Minn. Stat. §363A.44, the Contractor must have a current Equal Pay Certificate prior to Contract execution. If Contractor's Equal Pay Certificate expires during the term of this Contract, Contractor must promptly re-apply for an Equal Pay Certificate with the Minnesota Department of Human Rights and notify the State's Authorized Representative once the Contractor has received the renewed Equal Pay Certificate. If Contractor claims to be exempt, the State may require Contractor to verify its exempt status.

24. Workers' Compensation Insurance.

If applicable pursuant to Chapter 176, Contractor must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, Contractor will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State, including Coverage B, Employer's Liability. Insurance minimum limits are as follows:

\$100,000 – Bodily Injury by Disease per employee
\$500,000 – Bodily Injury by Disease aggregate
\$100,000 – Bodily Injury by Accident

If Minn. Stat. § 176.041 exempts Contractor from Workers' Compensation insurance or if the Contractor has no employees in the State, Contractor must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes Contractor from the Minnesota Workers' Compensation requirements.

If during the course of the contract the Contractor becomes eligible for Workers' Compensation, the Contractor must comply with the Workers' Compensation Insurance requirements herein and provide the State with a certificate of insurance.

25. **Artificial Intelligence.** Contractor agrees not to use access, or process any data provided by or on behalf of MSRS, or data generated through MSRS's use of the Cloud Services, for the purpose of training, testing, or developing machine learning models, artificial intelligence systems, or similar technologies.

26. **Security.** Contractor agrees to the MSRS Security Requirements.

26.1 Technical/Network Support

Provide access to MSRS employees to a system to track complaints and progress on problem resolution throughout the process. Changes to workflows and systems will be communicated in a timely fashion with enough lead time to allow MSRS to react appropriately. MSRS business personnel are available during non-peak times with advance notice.

Any work requiring downtime of system equipment will not be done during standard business hours of 6:30 a.m. – 5:00 p.m., CST, Monday through Friday. These changes must be communicated to and pre-approved by MSRS staff in accordance with MSRS change-management practices. VPN access is provided to authorized users outside the standard work hours. The work hours may be adjusted at the mutual agreement of the parties.

Consents to background checks for employees who will have on-site access and will restrict employee access to only persons authorized by State following a successful background check.

If connections are required between MSRS and Contractor systems, vendor will support a site-to-site VPN between systems. Vendor will work with MSRS to build test data.

26.2 Security Program

Must make all commercially reasonable efforts to protect and secure the MSRS data related to this Agreement. Will establish and maintain an information security program. The Contractor's program and relevant policies must align with appropriate industry security frameworks and standards such as National Institute of Standards and Technology ("NIST") 800-53 Special Publication Revision 4, Federal Information Processing Standards ("FIPS") 199, Federal Risk and Authorization Management Program ("FedRamp"), International Standard for Organization's ISO 27001, or Control Objectives for Information and Related Technology ("COBIT"). The contractor must also maintain a disaster recovery plan.

Will make non-confidential information regarding its security available to the MSRS on a confidential, need-to-know basis, along with other related non-confidential information reasonably requested by the MSRS regarding security practices and policies. Unless inconsistent with applicable laws, the Contractor and MSRS must treat the Contractor's policy and related information on security practices and policies that are specific to MSRS as confidential information and as not public data pursuant to Minnesota Statutes section 13.37.

26.3 Data Ownership

MSRS solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all MSRS data. The Contractor has no and acquires no right, title or interest, whether express or implied, in and to MSRS data. For purposes of this section, "data" has the meaning of "government data" in Minnesota Statutes section 13.02, subdivision 7. The term "MSRS confidential data" means all nonpublic information provided by the MSRS in connection with this Agreement, and the term "MSRS PII" means personally identifiable information of participants in MSRS Plans. The Contractor has no and acquires no right, title or interest, whether express or implied, in and to the MSRS data. For clarification, the term "MSRS data" shall not include Contractor IP.

Will only use MSRS data for the purposes set forth in the Agreement. Will only access MSRS data as necessary for performance of this Agreement. Will not access MSRS user accounts except to respond to service or technical problems or at MSRS specific request.

All MSRS data, including copies, summaries and derivative works thereof, must be remitted, in a mutually agreeable format and media, to MSRS by the Contractor upon request or upon completion, termination or cancellation of the Agreement. The foregoing sentence does not apply if the MSRS Chief Information Security Officer or designee authorizes in writing the Contractor to sanitize and/or destroy the data and certifies in writing the sanitization and/or destruction of the data. Within ninety days following any remittance of MSRS data to MSRS,

Contractor shall, unless otherwise instructed by the MSRS in writing, sanitize and/or destroy any remaining data and certify in writing that the sanitization and/or destruction of the data has occurred. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

In the event Contractor receives a request to release any MSRS data, the Contractor must immediately notify the MSRS Executive Director or designee. MSRS will give the Contractor instructions concerning the release of the data to the requesting party before the data is released. Must comply with the MSRS's instructions. The civil remedies of Minnesota Statutes section 13.08 apply to the release of the data by the Contractor.

26.4 Data Access

Must provide all MSRS locations with web-based access to the Contractor including imaged data records. MSRS will require appropriate access for staff to process transactions. Background checks are required for all agents, employees, and subcontractors who will be requiring system access and data at MSRS. Please note that background checks for non-US citizens may take up to six (6) weeks and vendors should plan this into the overall schedule.

26.5 Data Management

The Contractor is prohibited from using MSRS data for purposes outside the terms of the Agreement without prior consent. Including but not limited to; testing, development, and use in training generative artificial intelligence. Must maintain procedures to logically segregate MSRS data. Prior consent requires authorization in writing by the MSRS Chief Information Security Officer or designee must maintain and report as requested an audit trail of all system and transactional changes.

26.6 Data Encryption

Must encrypt all MSRS data at rest and in transit, in compliance with FIPS Publication 140-2 or applicable law, regulation or rule, whichever is a higher standard. All encryption keys must be unique to MSRS data. Will secure and protect all encryption keys to MSRS data. Encryption keys to MSRS data will only be accessed by the Contractor as necessary for performance of the Contract.

26.7 Data Storage

Agrees that any and all MSRS data will be stored, processed, and maintained solely on designated servers and that no such data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is encrypted and used as part of the Contractor's designated backup and recovery processes.

26.8 Data Center and Monitoring/Support Locations

During the term of the Contract, the Contractor agrees to: (1) locate all production and disaster recovery data centers that store, process or transmit MSRS data only in the continental United States, (2) store, process and transmit MSRS data only in the continental United States, and (3) locate all monitoring and support of all the services only in the continental United States. In order to perform due diligence, MSRS has the right to on-site visits and reasonable inspection of the data centers and computing environments with reasonable notice.

26.9 Security Audits & Remediation

Will audit the security of the systems and processes used to provide any and all services that support this Agreement, including those of the data centers used by Contractor to provide any and all services to the MSRS. This security audit: (1) will be performed at least once every calendar year; (2) will be performed according Statement on

Standards for Attestation Engagements ("SSAE") 16 Service Organization Control ("SOC") 2, International Organization for Standardization ("ISO") 27001, or FedRAMP; (3) will be performed by third party security professionals at Contractor's election and expense; (4) will result in the generation of an audit report ("Contractor Audit Report"), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section.

Upon the MSRS's reasonable, advance written request, the Contractor will provide to MSRS a copy of the Contractor Audit Report.

Will make best efforts to remediate any control deficiencies identified in the Contractor Audit Report in a mutually agreed upon timeframe.

If MSRS becomes aware of any other Contractor controls that do not substantially meet the MSRS requirements, MSRS may request remediation from the Contractor. Will make best efforts to remediate any control deficiencies identified by the MSRS or known by the Contractor, in a mutually agreed upon timeframe.

26.10 Security Incidents

If the Contractor becomes aware of or has reasonable suspicion of a privacy incident or security incident regarding any MSRS data, the Contractor must report such incident to the MSRS and the MSRS Chief Information Security Officer as soon as possible, but no later than twenty-four (24) hours after such incident. The decision to notify the affected data subjects and the form of such notice following report of a privacy incident or security incident will be in collaboration with MSRS. Notwithstanding anything to the contrary in this Agreement, Contractor will indemnify, hold harmless and defend MSRS and its officers, and employees for and against any claims, damages, costs and expenses related to any privacy incident or security incident involving any MSRS data. For purposes of clarification, the foregoing sentence shall in no way limit or diminish Contractor's obligation(s) to indemnify, save, hold harmless, or defend the MSRS under any other term of this Agreement. Will reasonably mitigate any harmful effects resulting from any privacy incident or security incident involving any MSRS data.

For purposes of this sub-section, "Security Incident" means the successful unauthorized access, use, disclosure, modification or destruction (without availability of backup copies) of MSRS Confidential Data or MSRS PII. For purposes of this sub-section, "Privacy Incident" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13) and/or federal privacy requirements in federal laws, rules and regulations by the Contractor. To the extent set forth in such Minnesota Government Data Practices Act this includes, but is not limited to, improper or unauthorized use or disclosure of not public data, improper or unauthorized access to or alteration of public data, and incidents in which the confidentiality of the data maintained by the Contractor has been breached. For purposes of this section, "not public data" has the meaning in Minnesota Statutes section 13.02, subdivision 8a.

26.11 Security Breach

A security breach shall be defined as the unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of certain MSRS data comprising MSRS participant data or MSRS PII maintained by MSRS or the Contractor. In the event that a security breach occurs, upon reasonable investigation and confirmation by the Contractor that MSRS data is impacted with respect to such data maintained by the Contractor, or upon determination that a breach has likely occurred if confirmation is not possible, shall promptly notify MSRS that a breach may have occurred and provide such reasonable information as the Contractor has obtained at such point in the investigation. In addition, shall on an ongoing basis continue to communicate additional information to MSRS regarding such breach as such information becomes available to the Contractor, provided that such information does not put the Contractor at further risk of any compromise to its security. Agrees to investigate and remediate the breach, and to communicate the results of the remediation to MSRS.

26.12 Subcontractors and Third-Parties

Agrees that no MSRS data shall be transmitted, exchanged or otherwise provided to other parties, except specifically agreed to in writing by the MSRS Authorized Representative. Must ensure that any contractors, subcontractors, agents and others to whom it provides MSRS data, agree in writing to be bound by the restrictions and conditions reasonably commensurate with the terms of this Agreement that apply to the Contractor and to the extent applicable to the services provided by such third parties with respect to MSRS data. Acknowledges and agrees that it is responsible for compliance with the terms of this Article by any of Contractor's subcontractors, agents or affiliates to whom it provides MSRS data.

26.13 Compliance with Data Privacy and Security Laws and Standards

Shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations. Service will provide security controls necessary to prevent unauthorized access to or use of the system, data, and images.

Shall establish appropriate administrative, technical, and physical safeguards designed to protect any and all MSRS data and to ensure the confidentiality, integrity, and availability of the data. This will include Personally Identifiable Information (PII) of MSRS Participants or other sensitive proprietary data as owned by MSRS. At a minimum, this shall include policies and standards for information ownership, identification and authentication, access control, physical and environmental security, system and application security, incident response, and training and awareness.

MSRS may view, but not remove, the current contents of Contractor's security policies and procedures during an annual in-person meeting at Contractor's headquarters or primary office location.

26.14 Physical Security

Shall employ reasonable physical security safeguards for systems involved in processing or storage of MSRS Participant Personally Identified Information (PII) to prevent the unauthorized access, disclosure, modification, destruction, use, etc., and to otherwise protect the confidentiality and ensure use conforms to Information Securities Policies and Standards.

26.15 System Maintenance & Application Development

Information systems will be configured to industry security best practices, such as Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST). Systems and applications will be patched in a timely manner so critical security and operational patches and fixes are implemented to ensure the confidentiality, integrity and availability of the information system.

Warrants that all services provided are free from any and all defects in materials, workmanship, and design. Warrants that all services provided are free from any and all viruses, malware, and other harmful or malicious code. Must scan all source code for vulnerabilities, including before and after any source code changes are made and again before being placed into production, and must promptly remediate any and all vulnerabilities. Must follow best practices for application code review and the most current version of the OWASP top 10.

26.17 Return of Equipment and Media

If applicable, MSRS-owned equipment and data storage identified as such by MSRS in the possession of the Contractor shall be returned to MSRS within a reasonable period after completion of the contract or project, or at the request of MSRS' Authorized Representative.

26.18 Contractor Employees and Agents

Shall require that its employees and agents who provide services hereunder or who have access to information or data acquired or generated hereunder to comply with Contractor's employee policies and procedures, which include protection of confidential information. Shall be responsible to cause its employees to comply with the Contractor's obligations to comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, as applicable to the Services.

26.19 Fraud/Identity Theft

If a Participant's personal information is compromised by any of the following:

- The Contractor
- Third-parties contracted by the Contractor
- Sub-contractors or affiliates of the Contractor

Contractor will notify MSRS as soon as practicable after the breach is known. This applies to all services under this contract. Will work with MSRS to resolve the participant-related issues as they pertain to fraud or identity theft, including but not limited to participant notifications and credit monitoring.

26.20 Business Continuity Planning

MSRS requires that the Contractor have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that services provided shall be maintained continuously in the event of a disruption to the operations, regardless of the cause of the disruption. Such plans must, at a minimum, define the Contractor's actions to address the impacts of the following key areas likely to cause a disruption to the Contractor's operations: loss of key personnel, loss of facility, and loss of information technology. Must conduct testing and review of its business continuity and disaster recovery plan at least annually. Upon MSRS request, the Contractor must also participate, at mutually agreed upon times, in MSRS business continuity and disaster recovery testing, training, and exercise activities. A successful exercise of full call transfer from MSRS to the Contractor is to be conducted annually, and duplicate records in connection with the plans are maintained by Contractor off-site to reconstruct necessary data.

27. Survival of Terms.

The following clauses survive the expiration or cancellation of this Contract: Indemnification; State Audits; Government Data Practices; Intellectual Property; Publicity and Endorsement; Governing Law, Jurisdiction, and Venue; and Data Disclosure. Any other Contract term that expressly states or by its nature shall survive, shall survive.

Exhibit A, Supplement 1

IT TERMS

1. Supply Chain Security.

Notwithstanding anything else in this Section, this Section does not and shall not limit any other rights of the State under this Contract, including, but not limited to, warranties, acceptance, and return policy, if any.

- 1.1 Security Practices and Preventive Controls. The Contractor will use reasonable commercial efforts to ensure that the Contractor and any subcontractors or third parties involved in assembling, manufacturing, packaging, distributing, handling, warehousing, transporting or shipping State goods, including goods intended to be but not yet delivered to the State, meet all applicable security standards and all applicable local, state, federal, and international laws, rules and regulations (hereinafter "supply chain security").

Contractor must maintain certification/accreditation in an official supply chain security program and comply with that program's security standards for all orders sourced from the Contract. Official supply chain security program is defined as one of the following: ISO 28000 or 27036 (as applicable), SAE AS5553 or other SAE standard (as applicable), Customs-Trade Partnership Against Terrorism (C-TPAT), Authorized Economic Operator (AEO), or other program accepted in writing by the State, MSRS IT ITOps@mnretire.gov and the State, Department of Administration's Office of State Procurement ("OSP"). To demonstrate certification/accreditation, Contractor must provide to OSP and MSRS within one month following the effective date of this Contract or amendment adding this Section, whichever is later, a letter verifying its certification/accreditation in an official supply chain security program. Contractor will promptly notify OSP and MSRS of any change to its certification/accreditation.

Alternatively, if Contractor is not certified/accredited or loses certification/accreditation, Contractor must complete a MSRS security form to confirm that it complies with supply chain security. The form will require supporting documentation of any responses and must be completed to MSRS's satisfaction.

- 1.2 Notification of Supply Chain Security Breach. Contractor will promptly notify OSP, MSRS, and the ordering entity, if different from MSRS, of any breach of supply chain security involving State goods, including goods intended to be but not yet delivered to the State. Breach of supply chain security includes, but is not limited to, cargo theft, tampering, unauthorized access, or other activities that involve suspicious actions or circumstances. Goods received with viruses, malware or similar security deficiencies constitute breach of supply chain security.
- 1.3 Return/Rejection of Goods. Notwithstanding anything to the contrary, if a breach of supply chain security has occurred or the State in good faith suspects a breach may have occurred, including evidence that packaging or goods were tampered with or damaged, the State may reject delivery of those goods or return any of those goods already delivered. Breach of supply chain security has the meaning described in the preceding Subsection "Notification of Supply Chain Security Breach." Rejection of delivery or return of goods shall be solely the responsibility and at the cost and expense of the Contractor.

The State may sanitize or destroy components of the goods prior to returning the goods to Contractor or instruct Contractor to promptly sanitize or destroy goods upon their return. Following the completion of any such sanitization or destruction, and upon request by MSRS, the Contractor shall provide a Certificate of Data Destruction/Sanitization that meets the requirements of the then current version of NIST Special Publication 800-88 or DOD 5220.22-M Supplement. The Certificate of Data Destruction/Sanitization must be provided to MSRS, if requested, within one month following the return of the goods.

At no additional expense to the State, Contractor must provide within a reasonable time frame replacement goods for any goods that were rejected at delivery or returned due to a supply chain security breach. Any costs and expenses associated with removal or replacement of the goods, including sanitization and destruction costs and expenses, will be the responsibility of the Contractor.

Security and Data Protection. Contractor is responsible for the security and protection of State data subject to and related to Cloud Services in this Contract. The terms, conditions, and provisions of this Security and Data Protection section take precedence and will prevail over any other terms, conditions, and provisions of the Contract, if in conflict. This Security and Data Protection section, including its sub-sections, survives the completion, termination, expiration, or cancellation of the Contract.

For the purposes of this Security and Data Protection section, the following terms have the following meanings:

“Cloud Services” includes “cloud computing” as defined by the U.S. Department of Commerce, NIST Special Publication 800-145 (currently available online at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>) and any other software, hardware, hosting service, subscription, or other service or product by which Contractor stores, transmits, processes or otherwise has access to State data.

“State” means the State, or a cooperative purchasing venture (“CPV”) member when the CPV member is the ordering entity (if CPV purchases are permitted under this Contract).

“Data” has the meaning of “government data” in Minn. Stat. § 13.02, subd. 7.

“Not public data” has the meaning in Minn. Stat. § 13.02, subd. 8a.

"Security incident" means any actual, successful or suspected: (1) improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, modification of, alteration to, loss of, damage to or destruction of State data; (2) interference with an information system; (3) disruption of or to Contractor's service(s); or (4) any similar or related incident.

"Privacy incident" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); violation of federal data disclosure or privacy requirements in federal laws, rules and regulations; or breach of a contractual obligation to protect State data. This includes, but is not limited to, improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, damage to, loss of, modification of, alteration to or destruction of State data protected by such State or federal laws or by contract.

- 1.4 Data Ownership. The State solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all State data. Contractor has no and acquires no right, title or interest, whether express or implied, in and to State data.

Contractor will only use State data for the purposes set forth in the Contract. Contractor will only access State data as necessary for performance of this Contract. Contractor will not access State user accounts except to respond to service or technical problems or at the State's specific request.

All State data, including copies, summaries and derivative works thereof, must be remitted, in a mutually agreeable format and media, to the State by the Contractor upon request or upon completion, termination or cancellation of the Contract. The foregoing sentence does not apply if the State Chief Information Security Officer or delegate authorizes in writing the Contractor to sanitize or destroy the data and the Contractor certifies in writing the sanitization or destruction of the data. Within ninety days following any remittance of State data to the State, Contractor shall, unless otherwise instructed by the State in writing, sanitize or destroy any remaining data and certify in writing that the sanitization or destruction of the data

has occurred. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

In the event Contractor receives a request to release any State data, Contractor must immediately notify the State's data practices compliance official. The State will give Contractor instructions concerning the release of the data to the requesting party before the data is released. Contractor must comply with the State's instructions. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data by Contractor.

- 1.5 Notification of Incidents. If Contractor becomes aware of or has reasonable suspicion of a privacy incident or security incident regarding any State data, Contractor must report such incident to the State and the State Chief Information Security Officer as soon as possible, but no later than twenty-four (24) hours after such incident. The decision to notify the affected data subjects and the form of such notice following report of a privacy incident or security incident are the responsibility of the State. Notwithstanding anything to the contrary in this Contract, Contractor will indemnify, hold harmless and defend the State and its officers, and employees for and against any claims, damages, costs and expenses related to any privacy incident or security incident involving any State data. For purposes of clarification, the foregoing sentence shall in no way limit or diminish Contractor's obligation(s) to indemnify, save, hold harmless, or defend the State under any other term of this Contract. Contractor will reasonably mitigate any harmful effects resulting from any privacy incident or security incident involving any State data.

- 1.6 Security Program. Contractor will make best efforts to protect and secure the State data related to this Contract. Contractor will establish and maintain an Information Security Program ("Program") that includes an information security policy applicable to any and all Cloud Services ("Policy"). Contractor's Program and Policy must align with appropriate industry security frameworks and standards such as National Institute of Standards and Technology ("NIST") 800-53 Special Publication Revision 4, Federal Information Processing Standards ("FIPS") 199, Federal Risk and Authorization Management Program ("FedRamp"), or Control Objectives for Information and Related Technology ("COBIT").

Upon the State's request, Contractor will make its Policy available to the State on a confidential, need-to-know basis, along with other related information reasonably requested by the State regarding Contractor's security practices and policies. Unless inconsistent with applicable laws, Contractor and the State must treat the Policy and related information on security practices and policies that are specific to the State as confidential information and as not public data pursuant to Minn. Stat. § 13.37.

- 1.7 Data Management. Contractor will not use State data, including production data, for testing or development purposes unless authorized in writing by the State Chief Information Security Officer or delegate. Contractor will implement and maintain procedures to physically and logically segregate State data, unless otherwise explicitly authorized by the State Chief Information Security Officer or delegate.
- 1.8 Data Encryption. Contractor must encrypt all State data at rest and in transit, in compliance with FIPS Publication 140-2 or applicable law, regulation or rule, whichever is a higher standard. All encryption keys must be unique to State data. Contractor will secure and protect all encryption keys to State data. Encryption keys to State data will only be accessed by Contractor as necessary for performance of this Contract.
- 1.9 Data Storage. Contractor warrants that any and all State data will be stored, processed, and maintained solely on designated servers and that no such data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is in use as part of the Contractor's designated backup and recovery processes.

- 1.10 Data Center and Monitoring/Support Locations. During the term of the Contract, Contractor will: (1) locate all production and disaster recovery data centers that store, process or transmit State data only in the continental United States, (2) store, process and transmit State data only in the continental United States, and (3) locate all monitoring and support of all Cloud Services only in the continental United States. The State has the right to on-site visits and reasonable inspection of the data centers upon notice to Contractor of seven calendar days prior to visit.
- 1.11 Security Audits & Remediation. Contractor will audit the security of the systems and processes used to provide any and all Cloud Services, including those of the data centers used by Contractor to provide any and all Cloud Services to the State. This security audit: (1) will be performed at least once every calendar year beginning with 2016; (2) will be performed according Statement on Standards for Attestation Engagements (“SSAE”) 16 Service Organization Control (“SOC”) 2, International Organization for Standardization (“ISO”) 27001, or FedRAMP; (3) will be performed by third party security professionals at Contractor’s election and expense; (4) will result in the generation of an audit report (“Contractor Audit Report”), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section.

Upon the State’s reasonable, advance written request, Contractor will provide to the State a copy of the Contractor Audit Report.

Contractor will make best efforts to remediate any control deficiencies identified in the Contractor Audit Report in a commercially reasonable timeframe.

If the State becomes aware of any other Contractor controls that do not substantially meet the State’s requirements, the State may request remediation from Contractor. Contractor will make best efforts to remediate any control deficiencies identified by the State or known by Contractor, in a commercially reasonable timeframe.

- 1.12 Insurance and Liability. Contractor warrants that it has and will maintain the insurance described below in force and effect throughout the term of the Contract. An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor’s policy limits to satisfy the full policy limits required by the Contract provided that Contractor warrants that the minimum coverage requirements below are met.

Professional/Technical, Errors and Omissions, including Network Security and Privacy Liability Insurance (or equivalent Network Security and Privacy Liability coverage endorsed on another form of liability coverage or written as a standalone policy):

This policy must provide coverage for all claims Contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to the Contract, including but not limited to claims which may arise from failure of Contractor’s or a subcontractor’s security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of confidential or private information, transmission of a computer virus or denial of service.

Contractor is required to carry the following minimum limits:

\$2,000,000 – per claim or event
\$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the Contractor and, unless Contractor maintains an audited net worth of at least \$100 million, the deductible may not exceed \$100,000 without the written approval of

the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources. The retroactive or prior acts date of such coverage shall not be after the effective date of the Contract. Contractor shall maintain such insurance for a period of at least three (3) years following expiration or termination of the Contract. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract. If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor will notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State. Contractor is responsible for payment of Contract related insurance premiums and deductibles. If Contractor is self-insured, a Certificate of Self-Insurance must be provided to the State. Contractor shall obtain insurance policy(ies) from insurance company(ies) having an "AM BEST" rating of A- (minus); Financial Size Category ("FSC") VII or better, and authorized to do business in the State. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's authorized representative upon written request. The State reserves the right to immediately terminate the Contract if the Contractor is not in compliance with the insurance requirements of this sub-section and retains all rights to pursue any legal remedies against the Contractor.

Notwithstanding any limitation of liabilities in the Contract, the Contractor shall be liable for all damages to the extent such damages are within the insurance limit.

- 1.13 Subcontractors and Third Parties. Contractor warrants that no State data will be transmitted, exchanged or otherwise provided to other parties except as specifically agreed to in writing by the State Chief Information Security Officer or delegate. Contractor must ensure that any contractors, subcontractors, agents and others to whom it provides State data, agree in writing to be bound by the same restrictions and conditions under this Contract that apply to Contractor with respect to such data.
- 1.14 Compliance with Data Privacy and Security Laws and Standards. Contractor shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations.
- 1.15 Remedies. Contractor acknowledges that the State, because of the unique nature of its data, would suffer irreparable harm in the event that Contractor breaches its obligation under this Security and Data Protection section, and monetary damages may not adequately compensate the State for such a breach. In such circumstances, the State will be entitled, in addition to monetary relief, to injunctive relief or specific performance as may be necessary to restrain any continuing or further breach by Contractor, without showing or proving any actual damages sustained by the State.
- 1.16 Business Continuity. Contractor shall have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that Cloud Services provided under this Contract shall be maintained continuously in the event of a disruption to the Contractor's operations, regardless of the cause of the disruption. Such plans must, at a minimum, define the Contractor's actions to address the impacts of the following key areas likely to cause a disruption to Contractor's operations: loss of key personnel, loss of facility, and loss of information technology. Contractor must conduct testing and review of its business continuity and disaster recovery plan at least annually. Upon State request, Contractor must also participate, at mutually agreed upon times, in State business continuity and disaster recovery testing, training, and exercise activities.

Any term or condition that allows the Contractor to terminate the Contract for any or no reason (i.e., termination for convenience) is null and void. In the event of termination or cancellation of this Contract for any reason, the Contractor shall continue to provide any then-existing Cloud Services for as long as the State needs to transfer its data, software and other assets to an alternate service or service provider. After any such termination or cancellation, the State may purchase the continuing Cloud Services at the pricing in effect prior to such termination or cancellation. The fee for any such purchase shall be prorated for the period of time needed, as determined by the State, and shall be reduced by the amount paid for Cloud Services that were not used prior to such termination or cancellation. The amount of any such fee reduction shall be determined on a pro-rata basis. The Contractor shall refund to the State any unused portion of payments for Cloud Services.

- 1.17 Background Checks. Contractor represents that it has conducted and will conduct background investigations into all of Contractor's agents, employees, and subcontractors that will provide Cloud Services to the State. Such background investigations must have been or will be conducted by investigating local, state and federal criminal records, local, state and federal civil case records, and employment references.

If any provision of this sub-section is found to violate any applicable laws, rules, or State policies, then the Contractor will be relieved of all obligations arising under such provision. Notwithstanding anything to the contrary in this sub-section, this sub-section is only applicable and effective to extent that it is consistent with applicable laws, rules, and State policies.

- 1.18 Secure Coding. Contractor warrants that all Cloud Services are free from any and all defects in materials, workmanship, and design. Contractor warrants that all Cloud Services are free from any and all viruses, malware, and other harmful or malicious code. Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made and again before being placed into production, and must promptly remediate any and all vulnerabilities. Contractor must follow best practices for application code review and the most current version of the OWASP top 10.

Exhibit B: Insurance Requirements

1. Notice to Contractor.

- 1.1 The Contractor is required to submit Certificates of Insurance acceptable to the State as evidence of insurance coverage requirements prior to commencing work under this Contract.
- 1.2 Contractor shall not commence work under the contract until they have obtained all the insurance described below and the State has approved such insurance. Contractor shall maintain such insurance in force and effect throughout the term of this Contract, unless otherwise specified in this Contract
- 1.3 The failure of the Contractor to provide a Certificate of Insurance, for the policies required under this Contract or renewals thereof, or failure of the insurance company to notify the State of the cancellation of policies required under this Contract shall not constitute a waiver by the State to the Contractor to provide such insurance.
- 1.4 The State reserves the right to immediately terminate this Contract if the Contractor is not in compliance with the insurance requirements and retains all rights to pursue any legal remedies against the Contractor. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's Authorized Representative upon written request.

2. Notice to Insurer.

- 2.1 The Contractor's insurance company(ies) waives its right to assert the immunity of the State as a defense to any claims made under said insurance.
- 2.2 Insurance certificate holder should be addressed as follows:

Minnesota State Retirement System
Attention Kris Wenner, Contract Manager
60 Empire Drive, Suite 300
St. Paul, Minnesota 55103-3000

Or send by email to: Kris.wenner@mnretire.gov

3. Additional Insurance Conditions. The following apply to the Contractor, or the Contractor's subcontractor:

- 3.1 Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract.
- 3.2 If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor agrees to notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State;
- 3.3 Contractor is responsible for payment of Contract related insurance premiums and deductibles;
- 3.4 If Contractor is self-insured, a Certificate of Self-Insurance must be attached;
- 3.5 Contractor's policy(ies) shall include legal defense fees in addition to its policy limits with the exception of professional liability.

- 3.6 Contractor's insurance companies must either (1) have an AM Best rating of A- (minus) and a Financial Size Category of VII or better, and be authorized to do business in the State of Minnesota or (2) be domiciled in the State of Minnesota and have a Certificate of Authority/Compliance from the Minnesota Department of Commerce if they are not rated by AM Best.
- 3.7 An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor's policy limits to satisfy the full policy limits required by the Contract.

4. **Coverages. Contractor is required to maintain and furnish satisfactory evidence of the following insurance policies:**

- 4.1 **Commercial General Liability Insurance.** Contractor is required to maintain insurance protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from claims for property damage, including loss of use which may arise from operations under the Contract whether the operations are by the Contractor or by a subcontractor or by anyone directly or indirectly employed by the Contractor under the contract. Insurance minimum limits are as follows:

\$2,000,000 – per occurrence

\$2,000,000 – annual aggregate

\$2,000,000 – annual aggregate – applying to Products/Completed Operations

The following coverages shall be included:

- Premises and Operations Bodily Injury and Property Damage
- Personal and Advertising Injury
- Blanket Contractual Liability
- Products and Completed Operations Liability
- **State of Minnesota named as an Additional Insured**, to the extent permitted by law

- 4.2 **Commercial Automobile Liability Insurance.** Contractor is required to maintain insurance protecting it from claims for damages for bodily injury as well as from claims for property damage resulting from the ownership, operation, maintenance or use of all owned, hired, and non-owned autos which may arise from operations under this contract, and in case any work is subcontracted the contractor will require the subcontractor to maintain Commercial Automobile Liability insurance. Insurance minimum limits are as follows:

\$2,000,000 – per occurrence Combined Single limit for Bodily Injury and Property Damage

In addition, the following coverages should be included: Owned, Hired, and Non-owned Automobile.

Evidence of Subcontractor insurance shall be filed with the Contractor.

- 4.3 **Workers' Compensation Insurance.** Statutory Compensation Coverage. Except as provided below, Contractor must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, Contractor will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State, including Coverage B, Employer's Liability. Insurance **minimum** limits are as follows:

\$100,000 – Bodily Injury by Disease per employee

\$500,000 – Bodily Injury by Disease aggregate

\$100,000 – Bodily Injury by Accident

If Minn. Stat. § 176.041 exempts Contractor from Workers' Compensation insurance or if the Contractor has no employees in the State, Contractor must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes Contractor from the Minnesota Workers' Compensation requirements.

If during the course of the contract the Contractor becomes eligible for Workers' Compensation, the Contractor must comply with the Workers' Compensation Insurance requirements herein and provide the State with a certificate of insurance.

- 4.4 **Professional Liability, Errors, and Omissions.** This policy will provide coverage for all claims the contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to Contractor's professional services required under the contract. Insurance **minimum** limits are as follows:

\$2,000,000 - per claim or event
\$2,000,000 - annual aggregate

Any deductible will be the sole responsibility of the Contractor and may not exceed \$50,000 without the written approval of the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources.

The retroactive or prior acts date of such coverage shall not be after the effective date of this Contract and Contractor shall maintain such insurance for a period of at least three (3) years, following completion of the work. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

- 4.5 **Network Security and Privacy Liability Insurance (or equivalent).** [Include this insurance requirement when there are technology-related risks (e.g., software licenses, subscription services, maintenance and support services). Also, use when Contractor has access to not public data on state's network or on Contractor's network.] The coverage may be endorsed on another form of liability coverage or written on a standalone policy. Contractor shall maintain insurance to cover claims which may arise from failure of Contractor's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of not public data including but not limited to confidential or private information, transmission of a computer virus or denial of service. Insurance minimum limits are as follows:

\$2,000,000 per occurrence
\$2,000,000 annual aggregate

The following coverage shall be included: State of Minnesota named as an Additional Insured unless the coverage is written under a Professional Liability policy.

- 4.6 **Privacy Liability Insurance (or equivalent).** [Include this insurance requirement when there are no technology-related risks but Contractor has access to not public data that is not on a network (e.g., paper records).] The coverage may be endorsed on another form of liability coverage or written on a standalone policy. The Contractor shall maintain insurance to cover claims which may arise from failure of the Contractor to ensure the security of not public data stored on the State's documents, including but not limited to paper, microfilms, microfiche, magnetic computer tapes, cassette tapes, photographic negatives, photos, hard disks, floppy disks, and carbon sheets, while in the Contractor's care, custody, and control. Insurance minimum limits are as follows:

\$2,000,000 - Per Occurrence
\$2,000,000 - Annual Aggregate

The following coverage shall be included: State of Minnesota named as an Additional Insured unless the coverage is written under a Professional Liability policy.

- 4.7 **Property of Others Insurance (or equivalent).** [Include this insurance requirement when there is property owned by the state that is or may be in the Contractor's care, custody, and control. Please note this coverage should be used if the Contractor is removing the state property from state grounds.] The Contractor shall maintain a Property insurance policy covering "All Risk" of direct physical loss or damage, or equivalent, including the perils of theft, flood, transit, earthquake, and pollution clean-up expense for property owned by the state that is in the Contractor's care, custody, and control. Any deductible shall be the sole responsibility of the Contractor. Insurance **minimum** limits are as follows: The Contractor is solely responsible for the coverage equal to that of the actual cash value of state-owned property in the Contractor's care, custody, and control at any given point in time.

Exhibit C: Specifications, Duties, and Scope of Work

This page is “Intentionally Left Blank” for Contract Sample purposes. After the contract has been awarded to the selected contractor, the Specifications, Duties, and Scope of Work will be on this page as Exhibit C and it will become part of the actual, executed contract.

Exhibit D: Pricing

This page is “Intentionally Left Blank” for Contract Sample purposes. After the contract has been awarded to the selected contractor, the Price will be on this page as Exhibit D and it will become part of the actual, executed contract.