STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
700 GOVERNOR'S DRIVE
PIERRE, SOUTH DAKOTA 57501

Quality Improvement Coordination and Support
PROPOSALS ARE DUE NO LATER THAN MAY 4, 2023 by 5:00 PM CST.

23RFP8590 **BUYER**: Office of the Secretary **POC**: Kirsten Smart
Kirsten.Smart@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____ (Digital Signature allowed)

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

FEDERAL TAX ID#: _____ E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The South Dakota Department of Social Services (DSS) is dedicated to strengthening families to foster health, wellbeing, and independence. To support this mission, DSS has adopted a strategic plan which includes a goal to invest in continuous improvement of efficiencies, effectiveness, and technology by increasing the use of continuous improvement models to improve efficiencies and measure effectiveness.
See https://dss.sd.gov/docs/contactus/StrategicPlan.pdf.

DSS is seeking proposals to provide department-wide quality improvement coordination and supports. The vendor will ultimately support all divisions in identifying quality improvement processes and models which best meet needs. This will include researching processes currently used as well as conducting a scan of other options, working with each division to identify which model is best, and training staff to implement this model. Vendors will also provide ongoing support after models are implemented.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Department of Social Services is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota. The reference number for the transaction is 23RFP8590. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/keyresources/rfp.aspx for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding **Letter of Intent** to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal.

The letter of intent needs to be received by email no later than the date and time indicated in the Schedule of Activities and must be addressed to Kirsten.Smart@state.sd.us. Place the following, exactly as written, in the subject line of your email: **Letter of Intent for 23RFP8590.** Be sure to reference the RFP number in any attached letter or document.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	3/27/2023
Letter of Intent to Respond Due	4/06/2023
Deadline for Submission of Written Inquiries	4/06/2023
Responses to Offeror Questions	4/20/2023
SFTP Request Due	4/20/2023
Proposal Submission	5/04/2023 5:00 PM CST
Oral Presentations/discussions (if required)	5/11/2023

Anticipated Award Decision/Contract Negotiation 5/25/2023

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received by the South Dakota Department of Social Services by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

Proposals must be submitted as PDF's via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder no later than the date and time indicated in the Schedule of Activities by emailing Kirsten Smart at the email indicated on page one.

The subject line should be "23RFP8590 SFTP Request". The email should contain the name and the email of the person who will be responsible for uploaded the document(s).

Please note, offeror will need to work with their own technical support staff to set up an SFTP compatible software on offeror's end. While the State of South Dakota can answer questions, State of South Dakota is not responsible for the software required.

All proposals may be signed in ink or digitally by an officer of the offeror legally authorized to bind the offeror to the proposal and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 RESTRICTION OF BOYCOTT OF ISRAEL

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 CERTIFICATION RELATING TO PROHIBITED ENTITY

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, is not an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.10 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.11 VENDOR INQUIRIES

Vendors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the Schedule of Activities. Email inquiries must be sent to Kirsten.Smart@state.sd.us with the following wording, exactly as written, in the subject line: **Questions for 23RFP8590**.

The Department of Social Services (DSS) will respond to offerors' inquiries by posting offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than the date and time indicated in the Schedule of Activities. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.12 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information.

Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

Offerors may submit a redacted copy of their proposal when they respond though this is optional.

1.13 LENGTH OF CONTRACT

The length of this contract is expected to be two years beginning June 1, 2023, with an option to renew for an additional year.

1.14 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in Hughes County, State of South Dakota. The laws of South Dakota shall govern this transaction.

1.15 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include, at minimum, the State's standard terms and conditions as seen in Attachment A - contract.

The offeror should indicate in their response any issues they have with any specific contract terms in Attachment A. If the offeror does not indicate any contract term issues, then the State will assume the terms are acceptable.

The clauses from the **Bureau of Information and Telecommunications** (BIT) are included as Attachment B. Because we expect a wide range of proposed solutions, we have included the widest number of possible clauses. We fully expect that, depending on the nature of your solution, IT clauses may be modified or removed in the final contract.

3.0 SCOPE OF WORK

3.1 General: The South Dakota Department of Social Services is seeking a vendor to provide quality improvement expertise and support. All work must be aligned to and support implementation of the DSS Strategic Plan. The vendor will assist at least one program within each division in identifying quality improvement methodologies that meet the needs of each division to improve efficiencies and effectiveness. The vendor will also provide training, support, or related follow up activities to support staff with the knowledge and skills needed to apply the process or model.

The Department of Social Services organizational chart is found in Attachment C.

Bidders must have quality improvement experience and expertise to apply. However, there is no expectation of a certain quality improvement model or process. The proposal must clearly articulate what specific quality improvement expertise the vendor and identified staff members have. The ideal proposal will demonstrate experience in quality improvement in a public/governmental and/or social services setting. The Department does not have an expectation of workload or number of FTE for the scope of work. It is up to the vendor to propose how the work will be fulfilled and demonstrate how each deliverable will be met. The vendor may propose one individual or a team of individuals to fulfil the work but must include the qualifications of any personnel delivering services. The vendor must provide services that meet all deliverables within the scope of work. Proposals for one component or components, such as research or training, will not be accepted. DSS will allow the vendor to propose sub-contracts for additional expertise if needed.

DSS will accept a variety of quality improvement processes and implementation strategies. Examples of models currently in use include LEAN and Continuous Quality Improvement. Currently, there is no intention to adopt a department-wide model.

The proposer should plan to attend regularly scheduled meetings with DSS which may be virtual or in person. In addition to the general scope of work described above, the vendor will have responsibility in the following areas.

3.2 Research, Identification, and Selection: The proposed work will begin with a scan of the latest research to help understand best practices around quality improvement methodologies. The vendor will be required to meet with each division to identify strengths and needs and assist each division with identifying and selecting which process is best for their goals/needs. Information will need to be gathered and presented to a DSS team and must include a summary of the strengths and weaknesses of each of the models reviewed and how each relates to the goals/needs of each DSS division. The vendor should propose how they will collect this information and how the data will be presented. Final deliverables may include support materials for DSS and division level engagement.

The vendor will also assist in developing each division's quality improvement plans in accordance with the DSS Strategic Plan. Serve as a quality improvement liaison between the DSS Goal 2 Strategic Goal team and the broader South Dakota Department of Social Services quality initiatives. Include an approximate timeframe or timeline as to when this deliverable will be met.

3.3 Staff Support and Initial Training: The vendor will be expected to assist the Department in creating a culture of quality improvement in the Department of Social Services based on the nationally recognized quality improvement frameworks, tools, and methods. The vendor shall build capacity of DSS teams who will be piloting/implementing a quality improvement model, DSS supervisors, and DSS staff. The proposal should include the following, but is not limited to the identified requirements:

3.3.1 Working with Division staff at every level and across multiple program areas to conduct quality improvement training to build their capacity of their chosen quality improvement model.

3.3.2 Seek out best practices in quality improvement and share tools and materials with staff. Create a quality improvement toolkit for DSS supervisors to support their staff.

3.3.3 Increase quality improvement capacity for DSS by researching and designing a training that can be delivered through the State's Learning Management system.

In addition to including an approximate timeframe or timeline as to when this deliverable will be met, vendor should propose an initial training plan that explains approximately how many trainings will be required, how those trainings will be delivered, and other relevant details. Include known details on training materials. Also include how progress on implementation will be documented and reported.

3.4 Ongoing and Follow Up Support: In addition to the initial training required for staff to implement quality improvement methodologies, the vendor will provide follow up support through implementation and as needed. The proposal should include routine meetings with each Division team to support implementation, assist the team to develop an implementation plan as well as monitor and document progress. The proposal should include an approximate timeframe or timeline as to when this deliverable will be met.

3.5 Data Monitoring and Reporting: Work closely with appropriate DSS staff to monitor relevant performance measures and outcomes for the Quality Improvement Strategic Plan and suggest improvement in data collection, monitoring, and reporting. Identify or create metrics to monitor outcomes for DSS as an organization. Assist each division in implementation of their specific quality improvement process by identifying and creating metrics to monitor outcomes. Align quality improvement projects with existing division priorities and the DSS Strategic Plan. Include details in the proposed timeline or work plan demonstrating when metrics will be created (unless known at this time), how often metrics will be measured and reported, and other relevant details. See https://dss.sd.gov/docs/contactus/outcomes.pdf for more information about DSS goals and outcomes as reported to the South Dakota Legislature.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 Provide the following information related to at ***least*** three previous and current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. Provide this information as well for any service/contract that has been terminated, expired or not renewed in the past three years:

a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
b. Dates of the service/contract; and
c. A brief, written description of the specific prior services performed and requirements thereof.

4.2 The offeror must submit information that demonstrates their availability and familiarity with the locale in which the projects are to be implemented. This may include but is not limited to familiarity with quality improvement, familiarity with the

Department of Social Services, and familiarity with the scope of work.

4.3 The offeror must describe their proposed project management techniques.

4.4 The offeror must detail examples that document their ability and proven history in handling special project constraints.

4.5 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.6 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all their questions or comments regarding the RFP, the evaluation, etc. to the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.7 The offeror may be required to submit a copy of their most recent independently audited financial statements.

5.0 PROPOSAL RESPONSE FORMAT

5.1 Only a PDF copy shall be submitted.

5.2 As outlined in section 1.5 “SUBMITTING YOUR PROPOSAL” proposals shall only be submitted electronically via SFTP.

5.3 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.4 All proposals must be organized and tabbed with labels for the following headings. The suggested page limit for the Detailed Response section is 10 pages. The suggested page limit for the entire proposal (including resumes and other attachments) is 50 pages.

5.3.1 **RFP Form**. The State’s Request for Proposal form completed and signed.

5.3.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

5.3.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:

5.3.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.3.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 3 and 4. The offeror may include a work plan or timeline in each sub section of the 3.0 Scope of Work, or they may include a full project timeline/work plan below 3.6. The response should identify each requirement being addressed as enumerated in the RFP.

5.3.3.3 A clear description of any options or alternatives proposed.

5.3.4 **Cost Proposal.** Cost will be evaluated with the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

See section 7.0 for more information related to the cost proposal.

6.0 **PROPOSAL EVALUATION AND AWARD PROCESS**

6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

6.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

6.1.3 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

6.1.4 Cost proposal.

6.1.5 Availability to the project locale;

6.1.6 Familiarity with the project locale;

6.1.7 Proposed project management techniques; and

6.1.8 Ability and proven history in handling special project constraints.

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

6.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached or the agency terminates the contracting process.

6.5.3 Only the response of the vendor awarded work becomes public. Responses to work orders for vendors not selected and the evaluation criteria and scoring for all proposals are not public. Vendors may submit a redacted copy with the full proposal as stated in Section 1.12 Proprietary Information. SDCL 1-27-1.5 and See SDCL 1-27-1.5 and 1-27-1.6.

7.0 **COST PROPOSAL**

The Cost Proposal must be presented by deliverable with justification. There is no preferred format or cost proposal template. The vendor may propose a one-year or two-year budget. The cost proposal should be included with the full proposal. For purposes of determining the best value, the technical proposal is the top priority. However, as technical scores become closer, price will become more important. Vendors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

ATTACHMENT A – Contract

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
OFFICE OF THE SECRETARY

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
OFFICE OF THE SECRETARIAT
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant

Referred to as State

The State hereby enters into a contract (the "Agreement" hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT'S South Dakota Vendor Number is . Upon execution of agreement, Consultant will provide the State with Consultant's Employer Identification Number, Federal Tax Identification Number, or Social Security Number.

2. PERIOD OF PERFORMANCE:
   A. This Agreement shall be effective as of June 1, 2023 and shall end on May 31, 2024, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of request for proposal process, RFP #8590

3. PROVISIONS:
   A. The Purpose of this Consultant contract is:
      1. The South Dakota Department of Social Services (DSS) is dedicated to strengthening families to foster health, wellbeing, and independence. To support this mission, DSS has adopted a strategic plan which includes a goal to invest in continuous improvement of efficiencies, effectiveness, and technology by increasing the use of continuous improvement models to improve efficiencies and measure effectivemess.

      2. Does this Agreement involve Protected Health Information (PHI)? YES ( ) NO (X)
      If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to attachment) .

      3. The Consultant WILL ( ) WILL NOT (X) use state equipment, supplies or facilities.

      4. If WILL is indicated above, the following state equipment, supplies, or facilities will be used.

   B. The Consultant agrees to perform the following services (add an attachment if needed.):
      1. Provide department-wide quality improvement coordination and supports.

C. The State agrees to:

1. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26-2.

2. Will the State pay Consultant expenses as a separate item?
   YES ( ) NO (X)
   If YES, expenses submitted will be reimbursed as identified in this Agreement.

D. The TOTAL CONTRACT AMOUNT will not exceed **$.**

4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 30 days of the Agreement end date to receive payment for completed services. If a final bill cannot be submitted in 30 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities.

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this Agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
The Consultant agrees to abide by all applicable provisions of the following: Byrd Anti Lobbying Amendment (31 USC 1352), Executive orders 12549 and 12689 (Debarment and Suspension), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996 as amended, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009, as applicable; and any other nondiscrimination provision in the specific statute(s) under which application for Federal assistance is being made; and the requirements of any other nondiscrimination statute(s) which may apply to the award.

8. COMPLIANCE WITH EXECUTIVE ORDER 2020-01:

By entering into this Agreement, Consultant certifies and agrees that it has not refused to transact business activities, it has not terminated business activities, and it has not taken other similar actions intended to limit its commercial relations, related to the subject matter of this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott of divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. Consultant further agrees to provide immediate written notice to the State if during the term of this Agreement it no longer complies with this certification and agrees such noncompliance may be grounds for termination of this Agreement.

9. COMPLIANCE WITH EXECUTIVE ORDER 2023-02:
Contractor certifies and agrees that the following information is correct:

In preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, Contractor is not an entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02.

Contractor further agrees that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. Contractor further agrees to provide immediate written notice to the State if during the term of this Agreement it no longer complies with this certification and agrees such noncompliance may be grounds for termination of this Agreement.

10. RETENTION AND INSPECTION OF RECORDS:
The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.

11. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties.

12. TERMINATION:
This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Consultant breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time, with or without notice. Upon termination of this Agreement, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination. If termination for breach is effected by the State, any payments due to Consultant at the time of termination may be adjusted to cover any additonal costs to the State as a result of Consultant's breach. Upon termination the State may take over the work and may award another party a contract to complete the work contemplated by this Agreement. If the State terminates for a breach by Consultant and it is determined that the Consultant was not at fault, then Consultant shall be paid for eligible services rendered and expenses incurred up to the date of termination.

Any terms of this Agreement that would, by their nature or through the express terms of this Agreement, survive the expiration or termination of this Agreement shall so survive, including by not limited to the terms of sections 9, 10, 14, 21, 22, 25 and 29.

13. FUNDING:
This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Agreement will be terminated by the State upon five day written notice. Consultant agrees that termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State or any officer, agent or employee of the State and Consultant waives any claim against the same.

14. ASSIGNMENT AND AMENDMENTS:
This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

15. CONTROLLING LAW:
This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

16. SUPERCESSION:
All prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

17. IT STANDARDS:
Any service, software or hardware provided under this Agreement will comply with state standards which can be found at http://bit.sd.gov/standards/.

18. SEVERABILITY:
In the event that any provision of this Agreement shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this Agreement, which shall remain in full force and effect.

19. NOTICE:
Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

20. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

21. STATE'S RIGHT TO REJECT:
The State reserves the right to reject any person or entity from performing the work or services contemplated by this Agreement, who present insufficient skills or inappropriate behavior.

22. INDEMNIFICATION:
Consultant agrees to indemnify the State of South Dakota, its officers, agents, and employees, from and against all claims or proceedings for actions, suits, damages, liabilities, other lossess or equitable releif that may arise at least in part as a result of an act or omission in performing services under this Agreement. Consultant shall defend the State of South Dakota, its officers, agents, and employees against any claim, including any claim, action, suit, or other proceeding related to the claim. Consultant's obligation to idemnify includes the payment of attorney fees and other costs of defense. In defending the State of South Dakota, its officers, agents, and employees, Consultant shall engage other professionals, subject to the written approval of the State which shall not be unreasonably witheld. Notwithstanding the foregoing, the State may, in its sole discretion and at the expense of Consultant, engage attorneys and other professionals to defend the State of South Dakota, its officers, agents, and employees, or to assist Consultant in the defense. This section does not require Consultant to be responsible for or defend against claims or proceedings for damages, liabilities, lossess or equitable relief arising solely from errors or omissions of the State, its officers, agents, or employees.

23. INSURANCE:
Before beginning work under this Agreement, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement, including naming the State of South Dakota, its officers and employees as additional insureds, as set forth below. The Consultant, at all times during the term of this Agreement, shall maintain in force insurance coverage of the types and limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds, but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $1,000,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles. The insurance shall include coverage for owned, hired, and non-owned vehicles. The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

C. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota or federal law.

D. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.) The insurance policy shall name the State of South Dakota, its officers and employees, as additional insureds but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

24. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this Agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Agreement either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

25. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

26. CONFIDENTIALITY OF INFORMATION:
For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosed, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation or may be required to sign separate confidentiality agreements, and it will limit access to the confidential information and related work activities to employees that have executed such agreements.

27. REPORTING PROVISION:
Consultant agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

28. DAVIS-BACON ACT:

When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction").

29. COMPLIANCE WITH 40 U.S.C. 3702 AND 3704:
    Where applicable, all contracts awarded by the non-Federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5).

30. FUNDING AGREEMENT AND "RIGHTS TO INVENTION":
    If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the Consultant wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the Consultant must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

31. FORCE MAJEAURE:
    Notwithstanding anything in this Agreement to the contrary, neither party shall be liable for any delay or failure to perform under the terms and conditions of this Agreement, if the delay or failure is caused by war, terrorist attacks, riots, civil commotion, fire, flood, earthquake or any act of God, or any causes beyond the party's reasonable control provided, however that in order to be excused from delay or failure to perform, the party must act diligently to remedy the cause of such delay or failure and must give notice to the other party as provided in this Agreement as soon as reasonably possible of the length and cause of the delay in performance.

32. WAIVER OF BREACH:
    The waiver by either party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provisions in this Agreement.

33. HEADINGS:
    The headings in this Agreement are for convenience and reference only and shall not govern, limit, modify or in any manner affect the scope, meaning, or intent of the provisions of this Agreement.

34. AUTHORITY TO EXECUTE:
    Consultant represents and warrants that the execution, delivery, and performance of this Agreement has been duly authorized by Consultant and that no approval, authorization, or consent of any governmental or regulatory agency is required to be obtained in order for Consultant to enter into this Agreement and perform its obligations under this Agreement. If the Consultant is a corporation, said corporation is duly incorporated, validly existing, and in good standing under the laws of its state of incorporation and has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Agreement. If Consultant is an individual person, partnership, or other non-corporate entity, Consultant is authorized to conduct business in and is in good standing in each jurisdiction in which Consultant will conduct business in connection with this Agreement. Consultant has obtained all licenses, certifications, permits, and authorizations necessary to perform the services under this Agreement and currently is in good standing with all regulatory agencies that regulate any or all aspects of Consultant's performance of the services. Consultant will maintain all required certifications, licenses, permits and authorizations during the term of this Agreement at its own expense.

35. AUTHORIZED SIGNATURES**:**
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

Consultant Signature	Date
Consultant Printed Name	
State - DSS Division Director	Date
State - DSS Chief Financial Officer Jason Simmons	Date
State – DSS Cabinet Secretary Matthew K. Althoff	Date

State Agency Coding:

CFDA #				
Company				
Account				
Center Req				
Center User				
Dollar Total				

DSS Program Contact Person _____
Phone _____

DSS Fiscal Contact Person Contract Accountant
Phone 605 773-3586

Consultant Program Contact Person _____
Phone _____
Consultant Program Email Address _____

Consultant Fiscal Contact Person _____
Phone _____
Consultant Fiscal Email Address _____

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

CONTRACTOR CERTIFICATION REQUIRED BY SOUTH DAKOTA EXECUTIVE ORDER 2023-02

Section 1 Definitions. The words used in this Certification shall mean:

1.1. "Prohibited Entity," an organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, limited liability company, or other entity or business association, including all wholly-owned subsidiaries, majority-owned subsidiaries, parent companies, or affiliates, of those entities or business associations, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela;

1.2. "Executive Branch Agencies," each state agency, authority, bureau, board, commission, department, or institution of the State of South Dakota that is controlled by the Governor;

1.3. "Contract," any type of agreement by or on behalf of the State to sell or lease supplies or goods, or to provide services, professional services, construction, or public improvements, to the State in return for a fee, or any other form of compensation to be paid or provided by the State; and

1.4. "Contractor," a vendor, supplier, construction contractor, or subcontractor that has submitted a bid or offer for or has been selected to engage in providing goods or services to the State but does not mean a sole proprietorship or individual natural U.S. citizen.

Section 2. Certification. The undersigned hereby certifies to the State of South Dakota that:

2.1. The undersigned is not a Prohibited Entity.

2.2 If at any time after making this certification the undersigned becomes a Prohibited Entity, the undersigned will provide immediate written notice to all Executive Branch Agencies with whom the undersigned has a Contract. The undersigned understands and agrees that if the undersigned becomes a Prohibited Entity, Executive Branch Agencies may terminate any Contract with the undersigned.

2.3 The undersigned acknowledges and agrees that Executive Branch Agencies have the right to terminate a Contract with any Contractor that submits a false certification.

_____
Company

_____ _____
Title Signature Date

Page left intentionally blank for: PROFESSIONAL SERVICES RFP EXEMPTION FORM

ATTACHMENT B – Bureau of Information and Telecommunications (BIT) Contract clauses.

BIT is charged by the state with making sure that all technology used is compatible with State Standards. Also, that the data of our citizens is safeguarded. Because we do not know what methods an offeror will use to access data we have included the widest possible number of clauses.

Depending on your proposed solution certain of these clauses may not be needed and will be removed from the final contract.

1. **THIRD PARTY HOSTING**
   If the Consultant has the State's data hosted by another party the Consultant must provide the State, the name of this party. The Consultant must provide the State with contact information for this third party and the location of their data center(s). The Consultant must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the consultant changes from the Consultant hosting the data to a third-party hosting the data or changes third-party hosting provider, the Consultant will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

2. **SECURING OF DATA**
   All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

3. **SECURITY PROCESSES**
   The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.

4. **SCANNING AND AUDIT AUTHORIZATION**
   The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by Consultant for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Consultant provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

   The Consultant will also allow the State at the State's expense, not to include Consultant's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of Consultant's IT security safeguards for the system and its data. The State will work with the Consultant to arrange the audit at a time least likely to create workload issues for the Consultant and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

   Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of

any licensure agreements between the State and Consultant. In the event of conflicting language this clause supersedes any other language in this, or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Consultant and the State agree that scanning results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

5. PASSWORD PROTECTION

The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

6. **MOVEMENT OF PROTECTED STATE DATA**

Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The Consultant will ensure that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

7. BANNED SERVICES

The Consultant warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

8. MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS

If the Consultant is hosting on their system or performing Software as a Service where there is the potential for the Consultant and/or the Consultant's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Consultant's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

9. THREAT NOTIFICATION

Upon becoming aware of a credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor supplying product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Consultant will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Consultant.

10. **SECURITY INCIDENT NOTIFICATION**

For protected non-health information only. The Consultant will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policies (contact Kirsten Smart at Kirsten.Smart@state.sd.us for a copy.) The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a

third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Consultant shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Consultant. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Consultant will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Consultant must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

A. The Consultant shall notify the State Contact within twelve (12) hours of the Consultant becoming aware that a Security Incident has occurred.

   If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

C. At the State's discretion within ____ the consultant must provide to the State all data available including: (i) Name of and contact information for the Consultant's Point of Contact for the Security Incident: (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered: (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred: and, (vii) the nature of the technologies involved. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person consultant must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Consultant shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Consultant is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Consultant reasonably determines that the breach will not likely result in harm to the affected person. The Consultant shall document the determination under this section in writing and maintain the documentation for not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and consultant shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

11. **HANDLING OF SECURITY INCIDENT**

For Security Incidents of protected non-health information under the Consultant's control and at the State's discretion the Consultant will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Consultant will also:

(i) fully investigate the incident,
(ii) cooperate fully with the State's investigation of, analysis of, and response to the incident,
(iii) make a best effort to implement necessary remedial measures as soon as it is possible and,
(iv) document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Consultant and at the Consultant's expense the Consultant will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Consultant shall offer ____ years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Consultant, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense.

If the Consultant is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twelve (12) hours of the investigation report being completed. If the Consultant is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

12. **SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION**

Security Incident means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. The Consultant shall alert the State Contact within twelve (12) hours of a Security Incident and provide daily updates to the BIT contact at their request. The Parties agree that this alert does not affect the Consultant's obligations under the Business Associate Agreement or the requirements of 45 CFR 164.410. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Consultant to conduct a review or investigation within the scope and methodology determined by the State. At the State's discretion, the review or investigation may be performed by a third party at the Consultant's expense.

Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the consultant is responsible for the Security Incident, and where the State incurs any costs in the investigation, review or remediation of the Security Incident, the Consultant shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the consultant is

responsible for the Security Incident, the Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Consultant's services and/or product(s).

13. **ADVERSE EVENT**
The Consultant shall notify the State Contact within 2 days if the Consultant becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Consultant's actions or inactions. The State can require a risk assessment of the Consultant the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

14. **BROWSER**
The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion and Adobe Flash will not be used in the system, site, and/or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

15. **INFORMATION TECHNOLOGY STANDARDS**
Any service, software or hardware provided under this agreement will comply with state standards which can be found at *http://bit.sd.gov/standards/*

16. **SECURITY ACKNOWLEDGEMENT FORM**
The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as Attachment F The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Consultant by the State contact before work on the contract may begin. This form constitutes the agreement of Consultant to be responsible and liable for ensuring that the Consultant, Consultant's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy- Contractor (ITSP) attached to this Agreement as Attachment F Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Consultant does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Consultant's, Consultant's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Consultant or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Consultant's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Consultant and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

17. **BACKGROUND CHECKS**
The State requires all employee(s) of the Consultant, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of both the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two (2) to four (4)

weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Consultant, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Consultant with notice of this determination.

18. **SECURITY**

The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Consultant warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
    a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
    b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
    c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
    d. **Low-** Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.
B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

19. MALICIOUS CODE

A. The Consultant warrants that the service contains no code that does not support an application requirement.
B. The Consultant warrants that the service contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the service or any media on which the service is delivered any malicious or intentionally destructive code.

20. **DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION**

During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended

while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the Consultant shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant's intellectual property at risk. If the remedy, update or patch the Consultant proposes is unable to present software and or hardware that meets the State's requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State's satisfaction within thirty (30) days of the denial of access to or removal from the production system and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the Agreement may be terminated.

21. **MOVEMENT OF PRODUCT**
The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

22. USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE
The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

23. **LOAD BALANCING**
The State routinely load balances across multiple servers, applications that run on the State's computing environment. The Consultant's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Consultant's product to be load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

24. **LICENSE AGREEMENTS**
Consultant warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

25. WEB AND MOBILE APPLICATIONS

The Consultant's application is required to;

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
C. close all connections and close the application at the end of processing;
D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
E. have no code not required for the functioning of application;
F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
I. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Consultant's application;
K. access no data outside what is defined in the "About" information for the Consultant's application;
L. your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;
M. if any health or medical information is gathered or accessed by this application that is not protected by HIPAA and HITECH rules and regulations then the opening screen must state, in an easy to read font that the application is gathering and or accessing health and or medical information and the user's privacy is not protected by federal regulations;
N. any application to be used on a mobile device must be password protected.

If the application does not adhere to the requirements given above or the Consultant has unacceptable disclosures, at the State's discretion, the Consultant will rectify the issues at no cost to the State.

26. OFFSHORE SERVICES

The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

27. CONSULTANT'S SOFTWARE LICENSES

The Consultant must disclose to the State the license(s) for any third-party software and libraries used by the Consultant's product(s) ((and/or) in the project by the Consultant) covered under this agreement if the State will not be the license(s) holder. The Consultant is required to provide copies of the license(s) for the third-party software and libraries to the State. No additional software and libraries may be added to the project after the contract is signed without notifying the State and providing the licenses of the software and libraries. Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Consultant to fulfil the Consultant's commitments agreed to in this agreement is the responsibility of the Consultant, not the State.

28. CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for

handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, v) Security incident response, and vi) Protected Health Information.

29. DATA SANITIZATION

At the end of the project covered by this Agreement the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Consultant and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Consultant will use a process and procedure that does satisfy the State.

30. USE OF PORTABLE DEVICES

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Consultant's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

31. REMOTE ACCESS

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

32. CONFIDENTIALITY OF INFORMATION

For purposes of this paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or third party Consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this agreement. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities agree to return all information received from the State to State's custody upon the end of the term of this agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information shall not include information that:

(i) was in the public domain at the time it was disclosed to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities;

(ii) was known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction at the time of disclosure from the State;

(iii) that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;

(iv) was independently developed by the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without the benefit or influence of the State's information;

(v) becomes known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. Consultant acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

33. CYBER LIABILITY INSURANCE

The Consultant shall maintain cyber liability insurance with liability limits in the amount of $_____ to protect any and all State data the Consultant receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Consultant employees, whether the device is owned by the employee or the Consultant. If the Consultant has a contract with a third-party to host any State data the Consultant receives as part of the project under this agreement, then the Consultant shall include a requirement for cyber liability insurance as part of the contract between the Consultant and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-part Consultant. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Consultant shall furnish copies of insurance policies if requested by the State. The insurance will stay in effect for ____ years after the work covered by this agreement is completed.

34. SOFTWARE FUNCTIONALITY AND REPLACEMENT

The software licensed by the Consultant to the State provides the following functionality:

Describe the broad functionality of software product licensed.

The Consultant agrees that:

A. If in the opinion of the State the Consultant reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State shall be entitled to license such software product at no additional license or maintenance fee.

B. If in the opinion of the State the Consultant releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Consultant discontinues the licensed

product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

35. CONSULTANT ELECTION NOT TO RENEW CONTRACT OR TO INCREASE FEES

The Consultant is obligated to give the State one hundred and eighty (180) days written notice in the event the Consultant intends not to renew the contract or intends to raise any fees or costs associated with the Consultant's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract.

36. DATA PROTECTION

Protection of personal privacy and data shall be an integral part of the business activities of the Consultant to ensure there is no inappropriate or unauthorized use of State's data at any time. To this end, the Consultant shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

A. The Consultant shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Consultant applies to its own non-public data.

B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Consultant or any party related to the Consultant for subsequent use in any transaction that does not include the State.

C. The Consultant will not use such data for the Consultant's own benefit and, in particular will not engage in data mining of State's data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

37. LEGAL REQUESTS FOR DATA

Except as otherwise expressly prohibited by law, the Consultant will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Consultant seeking State data maintained by the Consultant;

B. Consult with the State regarding its response;

C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and

D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

38. EDISCOVERY

The Consultant shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Consultant shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

39. PASSWORD POLICIES

Password policies for all Consultant employees will be documented annually and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multifactor Authentication.

Contractor Agreement to Comply with BIT Information Technology Security Policy

Please return agreement to your designated BIT Contact

Pursuant to the terms of the Agreement between the Contractor and the State, the Contractor is required to sign this Contractor Agreement to Comply with the BIT Information Technology Security Policy (the "Policy") on behalf of its current and future employees who will be responsible for fulfilling the requirements of the Agreement. The Contractor is responsible for ensuring that each Contractor employee complies with all information security policies and procedures found within the Policy. By signature below, the Contractor hereby acknowledges and agrees to the following:

1. In providing services under a contract, the Contractor will use non-public State of South Dakota technology infrastructure or information;
2. The Contractor will protect technology and information assets of the State from unauthorized activities including but not limited to access, disclosure, modification, deletion, and usage;
3. The Contractor agrees to follow state and federal regulations in regard to confidentiality and handling of data;
4. The Contractor has read and agrees to abide by the Policy, which is attached to the Agreement;
5. The Contractor will discuss with a state contact any violation of the Policy;
6. The Contractor understands that any individual found to have violated the Policy is subject to privilege revocation and, at the State's discretion, may be considered a breach of the Agreement with the State;
7. Access to the technology infrastructure of the State or the State's information is a privilege which may be changed or revoked at the discretion of BIT management;
8. Access to the technology infrastructure of the State automatically terminates upon contract termination unless otherwise agreed upon in writing by the parties; and
9. The Contractor shall promptly report violations of the Policy to the State Contact and BIT Help Desk (605-773-4357).

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: The individual signing this form on behalf of their entire company affirms that he/she has the authority to commit the Contractor and all its employees to follow the terms of this agreement.

Contractor Signature	Date	BIT Contact	Date

Printed Contractor name and Company name

Attachment C
DSS Divisions