STATE OF SOUTH DAKOTA
Department of Human Services
SOUTH DAKOTA DEVELOPMENTAL CENTER
Hillsview Plaza, East Highway 34
c\o 500 East Capitol
Pierre, SD 57501-5070

Institutional Food Services for South Dakota Developmental Center - Redfield
PROPOSALS ARE DUE NO LATER THAN 5:00 PM CST 4/5/2024

RFP #: 24RFP10213 State POC: Shane Wright EMAIL: shane.wright@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

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)

South Dakota Developmental Center (SDDC) intends to secure food service operations that meet the needs and concerns of people with intellectual and/or developmental disabilities. SDDC is seeking a nutritional, high quality, cost effective, and innovative solution to the food service needs of the facility. The full achievement of the comprehensive goals of this program should result in a food service operation that will complement the mission of SDDC.

This RFP is designed to provide interested Offerors with sufficient basic information to submit proposals meeting minimum requirements but is not intended to limit a proposal's content or exclude any relevant or essential data. Offerors are at liberty and are encouraged to expand upon the specifications to evidence service capability under any agreement.

All participating Offerors shall agree to comply with all of the conditions, requirements and instructions of this RFP.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The SD Developmental Center is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Human Services. The reference number for the transaction is RFP # 24RFP10213. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.3 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	2/23/2024
Deadline for Submission of Written Inquiries/Questions	3/15/2024
Deadline for Completion of Site Visits (if requested)	3/15/2024
Responses to Offeror Questions	3/22/2024
Proposal Submission Deadline	4/05/2024
Anticipated Start of Contract Negotiation	4/12/2024

1.4 SITE VISITS

Offerors are strongly encouraged to visit the campus and tour the food service facilities prior to submitting their proposal. To schedule a site visit, contact Shane Wright at shane.wright@state.sd.us. Place the following, exactly as written, in the subject line of your email: Site Visit Request for RFP # 24RFP10213. All site visits must be completed by the date indicated in the Schedule of Activities. Failure to perform a site visit shall not relieve the offerors from any items and conditions of this RFP.

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received by the date and time indicated in the Schedule of Activities.

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

Proposals, including all attachments, should be submitted in Microsoft Word AND/OR a PDF (must be in searchable format) electronic format via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder by emailing Shane Wright at shane.wright@state.sd.us. The subject line should be “RFP # 24RFP10213 SFTP Request”. Offerors will mail one printed copy and one electronic copy (can be emailed) of each portion of their proposal.

The email should contain the name and the email of the person who will be responsible for uploading the document(s).
Please note, Offerors 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, the State of South Dakota is not responsible for the software required.
The cost proposal must be in PDF electronic format in a separate sealed envelope and labeled "Cost Proposal".

All proposals must 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. The sealed envelope should be marked with the appropriate RFP Number and Title. **Proposals should be addressed and labeled as follows:**

REQUEST FOR PROPOSAL #: 24RFP10213
PROPOSAL DUE: 4/5/2024
STATE POC: Shane Wright
South Dakota Developmental Center
17267 W. 3rd St.
Redfield, SD 57469

No proposal shall be accepted from, or no contract or purchase order shall be 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 regards to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 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 SDCL 5-18A. 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 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.

1.10 CERTIFICATION OF NO STATE LEGISLATOR INTEREST

Offeror (i) understands neither a state legislator nor a business in which a state legislator has an ownership interest may be directly or indirectly interested in any contract with the State that was authorized by any law passed during the term for which that legislator was elected, or within one year thereafter, and (ii) has read South Dakota Constitution Article 3, Section 12 and has had the opportunity to seek independent legal advice on the applicability of that provision to any Agreement entered into as a result of this RFP. By signing an Agreement pursuant to this RFP, Offeror hereby certifies that the Agreement is not made in violation of the South Dakota Constitution Article 3, Section 12.

1.11 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.

1.12 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after 5:00 PM on 4/5/2024. Inquiries must be emailed to shane.wright@state.sd.us with the subject line “RFP #24RFP10213”.

The Department of Human Services (DHS) will respond to offerors’ inquiries no later than 3/22/2024. For expediency, DHS 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.

1.13 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.

1.14 LENGTH OF CONTRACT

The term of the contract shall be for one to five years, beginning July 1, 2024. Contract can be done annually with the option to renew, in one (1) year increments, for up to four (4) total extensions at the State's discretion and by mutual agreement of the parties; or for the entire term.

1.15 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in the State of South Dakota, regardless of its choice of law provisions whether statutory or decisional. The laws of South Dakota shall govern this transaction.

1.16 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.

1.17 SDDC VISITS TO OFFEROR'S FACILITIES

Representatives from the State reserve the right to inspect the Offeror's facilities and other operations under the Offeror's management prior to award of this proposal.

1.18 PROFIT OR LOSS

Any profit or loss from food services resulting from this proposal and the subsequent contract shall remain with the Contractor.

1.19 CERTIFICATION OF INDEPENDENT PRICE DETERMINATION

By submission of this proposal, the Offeror certifies, and in the case of a joint proposal, each party thereto certifies as to its own organization, the following in connection with this RFP:

A. Independent Pricing

Prices and guarantees in this proposal have been arrived at independently, without consultation, communication, or agreement with any competitor for the purpose of restricting competition.

B. Disclosure

Unless otherwise required by law, the prices and guarantees which have been quoted in this proposal have not been knowingly disclosed by the Offeror prior to opening in the case of an advertised procurement or prior to award in the case of a negotiated procurement, directly or indirectly to any other Offeror or to any competitor.

C. Restriction of Competition

No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.

D. Proposal Signatory Authority

1. Responsibility

The individual signing the proposal is the person in the Offeror's organization responsible for the decision as to the prices being offered herein and that he/she has not participated, and will not participate, in any action contrary to this solicitation.

2. Agent Authorization

The individual signing the proposal is not the person in the Offeror's organization responsible for the decision as to the prices being offered herein, but he/she has been authorized in writing to act as agent for the persons responsible for such decisions and that he/she has the authority to certify that such person has not participated, and will not participate, in any action contrary to this solicitation and their agent does so certify; and that he/she has not participated, and will not participate, in any action contrary to this solicitation.

1.20 NEWS RELEASES

News releases pertaining to this procurement or any part of the proposal shall not be made without the prior written approval of the State.

1.21 EMPLOYMENT OF STATE AGENCY PERSONNEL

The Offeror will not engage the services of any persons while they are employed by the State during the process of preparing a response for this RFP.

1.22 FOOD SERVICE LICENSE

Offerors will be required to have a South Dakota Food Service license obtained through the South Dakota Department of Health.

2.0 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract resulting from this RFP will include the State's standard terms and conditions listed below, along with any additional terms and conditions negotiated by the parties.

2.1 The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.

2.2 The Contractor's services under this Agreement shall commence on _____ and end on ____, unless sooner terminated pursuant to the terms hereof.

2.3 The Contractor will use State equipment, supplies or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL ch. 5-26.

2.5 The Contractor agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as the result of performing services hereunder. This section does not require the Contractor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

2.6 The Contractor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:

The Contractor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1,000,000.00 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.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:

The Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1,000,000.00.

C. Business Automobile Liability Insurance:

The Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than $1,000,000.00 for each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles.

D. Worker’s Compensation Insurance:

The Contractor shall procure and maintain workers’ compensation and employers’ liability insurance as required by South Dakota law.

Before beginning work under this Agreement, Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor shall furnish copies of insurance policies if requested by the State.

2.7 While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third

parties, or which may otherwise subject Contractor or the State to liability. Contractor shall report any such event to the State immediately upon discovery.

Contractor'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. Contractor'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 Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.9 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is effected by the State, any payments due to Contractor at the time of termination may be adjusted to cover any additional costs to the State because of Contractor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for a default by Contractor it is determined that Contractor was not at fault, then the Contractor shall be paid for eligible services rendered and expenses incurred up to the date of termination.

2.10 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 law or federal funds reductions, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

2.11 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.

2.12 This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.13 The Contractor will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

2.14 The Contractor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Contractor 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 Contractor 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.

2.15 Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and

documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

2.16 The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor 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.

2.17 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 _____ on behalf of the State, and by and to_____, on behalf of the Contractor, 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.

2.18 In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof.

2.19 All other 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.

2.20 Exhibit B includes the contract clauses from the Bureau of Information and Telecommunications (BIT). 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, clauses may be modified or removed in the final contract.

There is also a list of technical questions, Security and Vendor Questions which is attached as Exhibit C, the offeror must complete. These questions may be used in the proposal evaluation. It is preferred that the offeror's response to these questions is provided as a separate document from the RFP response. If the offeror will be hosting the solution, the file name must be "(Your Name) Hosted Security and Vendor Questions Response". If the solution will be hosted by the State, the file must be named "(Your Name) Security and Vendor Questions Response State Hosted". If the solution is not a hosted solution, the file name must be "(Your Name) Security and Vendor Questions Response". If there are multiple non-hosted solutions, please provide some designation in the file name that indicates which proposal it goes to. This document cannot be a scanned document but must be an original. If the offeror elects to make the Security and Vendor Questions part of its response, the questions must be clearly indicated in the proposal's Table of Contents. A single numbering system must be used throughout the proposal.

3.0 BACKGROUND INFORMATION

The mission of the South Dakota Developmental Center (SDDC) is to provide comprehensive specialized services designed to enhance quality of life and community inclusion for people with Intellectual Disabilities and/or Developmental Disabilities. SDDC provides many services that may include but are not limited to: physical development and health, physical and occupational therapy, communication development services, behavioral and mental health services, life skills, vocational development, participation in leisure and recreational activities, and independent living skills and training.

Exhibit A includes average daily census for SDDC.

4.0 SCOPE OF WORK

The Contractor must comply with the requirements as detailed in Section 4 of the RFP. The State will provide staff, as it deems appropriate, to perform contract monitoring.

4.1 GENERAL REQUIREMENTS, REGULATIONS AND LAWS

The Contractor will comply with all federal, state, and local laws, regulations, ordinances, guidelines, permits, and requirements applicable to providing services pursuant to the Agreement, and will be solely responsible for obtaining current information on such requirements. The Contractor agrees to meet or exceed all dietetic and food service laws and ordinances as adopted by federal, state, and local authorities. These laws and ordinances must include, but not limited to:

A. Standards set forth under the Centers for Medicare & Medicaid Services (CMS), including 42 CFR Part 483 Conditions of Participation for Individuals with Intellectual Disabilities;

B. State of South Dakota Administrative Rules, Article 46:17, Chapter 46:17:05:06 Dietary Services;

C. South Dakota Department of Health and local laws, rules, and regulations as they apply to dietetic and food service operations in hospitals and related institutions;

D. Relevant facility policies and procedures; and

E. Policies and procedures of the facility and any governing body under which the facility may operate now or in the future.

4.2 PERSONNEL REQUIREMENTS

4.2.1 STAFFING

The Contractor must demonstrate they currently employ or can employ sufficient staff to manage the food service operations at SDDC. Staff employees shall be on duty for the efficient, prompt, and sanitary service of food based upon a written staffing plan. Deviations from the staffing plan will require written notification to the recipient institution and subject to its approval.

The Contractor shall supply SDDC with a complete list of employees, supervisors and management assigned to work areas at the start of the contract and as frequently thereafter as requested by the SDDC. The list of employees shall include related trainings, certifications and/or licensures held by each staff person working at SDDC. The list shall be reviewed annually and at any other time as requested by the SDDC.

Personnel of the Contractor shall observe and be subject to all regulations of the SDDC. Failure to do so may be grounds for the SDDC to recommend dismissal.

4.2.2 SERVICE DIRECTOR

The Contractor shall provide a qualified on-site Food Service Director experienced in health care facilities. This person must possess required certification/licensure and shall be subject to the approval of SDDC. The response must clearly detail the expected duties of the Food Service Director.

The contractor should provide best efforts to ensure that the Food Service Director assigned to the SDDC shall not be changed more than once per year unless mutually agreed and not without thirty (30) days advanced notice and replacement selection made is acceptable to and mutually agreed by the SDDC, unless they have left the company. This position should not remain vacant for a period to exceed thirty (30) days.

The Food Service Director shall have the full authority to work with designated representatives of SDDC. The Food Service Director shall have a demonstrated proficiency with maintaining a sanitary food service operation, menu development, internal accounting and controls, financial management, and personnel management and supervision. Candidates with a college degree and experience in correctional, healthcare and/or institutional food services in increasingly responsible positions are desired.

The Food Service Director shall be certified/licensed as a food service manager in any facility requiring a certification or licensure for operation of said food service. The Food Service Director shall make at least monthly inspections of food delivery sites to ensure standards are being met. These inspections shall be documented for quality control purposes.

4.2.3 REGISTERED DIETICIANS

SDDC is a Medicare/Medicaid certified state facility and is surveyed by the South Dakota Department of Health. SDDC requires a Registered Dietician (RD) that meet state and federal requirements. The RD shall visit the facility not less than quarterly for quality control and adherence to standards. These visits shall be documented and a written report issued to the recipient institution.

SDDC may, at its option, employ a RD that would otherwise be provided by the Contractor. In this case, SDDC will assume all responsibilities and obligations for employing the RD as well as the work output. If this option is exercised, the reimbursement to Contractor for services may be reduced by SDDC to offset costs.

4.2.4 HEADQUARTERS MANAGEMENT STAFF

The Contractor shall identify headquarters management staff by name that shall routinely review and inspect operations, fill staff vacancies, consult with the SDDC on current and future food service programs, and act with full authority on the Contractor's behalf in all matters pertaining to the specifications of the contract.

4.2.5 TRAINING GUIDELINES

The Contractor shall provide SDDC with the training guidelines that will be utilized for each employee classification and clients (if applicable). Prior to assuming their normal food service duties, all employees of the Contractor must complete any training required by SDDC that is pertinent to food service personnel.

4.2.6 BACKGROUND INVESTIGATIONS

Background investigations will be required on all new Contractor employees prior to their assignment at the SDDC. The background investigation shall be conducted by the Contractor. The Contractor will be responsible for the cost. The Contractor is responsible for ensuring that any staff assigned to SDDC have no disqualifying background information that would prohibit them from providing services in an ICF.

The State requires any person who has access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential or have access to secure facilities will have fingerprint-based background checks. These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. This requirement will extend to include any of the Contractor's subcontractors, agents, assigns, and affiliated entities' employees.

4.3 PROVISION OF MEALS

4.3.1 SDDC DAYS OF OPERATION

SDDC operates twenty-four (24) hours a day, every day of the year, including weekends and holidays. The Contractor shall demonstrate they can provide meals every day SDDC is in operation, to include an emergency meal plan in the event of a catastrophic event that disrupts regular meal service.

4.3.2 FREQUENCY OF MEALS

The Contractor shall provide meals at least three (3) times per day with a minimum of two (2) hot meals per day. Regular mealtimes will be established with no more than fourteen (14) hours between a substantial evening meal and the following day's breakfast meal.

4.3.3 MEAL SCHEDULE AND SERVICE TIMES

The Contractor must develop a meal schedule specific to the needs of SDDC, although the meal schedule can be mutually agreed upon by both the Contractor and SDDC. Meal service times shall be reviewed and approved at least annually by SDDC. The Contractor is responsible to have meals ready to service during those times.

4.3.4 SERVING MEAL

Generally, mealtimes conform to the norms of the community, however the clients' schedules and preferences may result in slight variations. Clients may be served meals in a tray line or may be provided servings handed out in individual containers (except those receiving a sack lunch) in the Food Services building on the grounds of SDDC. The majority of clients eat at the SDDC Food Service Building. Some clients may receive their meals at their respective living areas. Food carts are loaded and delivered to the living areas located on the SDDC campus. Food must be served in appropriate quantity at appropriate temperature; in a form consistent with the developmental level of the client; and with appropriate utensils.

4.3.5 REQUISITION OF FOOD SUPPLIES BY AREA

Each living area can requisition bulk food supplies for snacks on a weekly basis. Snacks should be balanced between fresh fruits/vegetables and whole grain items as well as more traditional snack items.

Each living area can requisition supplies for one "special meal" per month. In this circumstance, the supplies are provided by the Contractor and SDDC staff are responsible for food preparation. Likewise, each living area can requisition supplies for one special event per month. The supplies are provided by the Contractor and SDDC staff are responsible for food preparation.

The Activity Center may have one large group activity per month. The Contractor is expected to provide cake, cookies, etc. for this activity.

4.3.6 SACK LUNCHES

The Contractor must provide a sack lunch to clients who miss a regularly scheduled meal through no fault of their own. The sack lunch shall meet the nutritional needs of the clients and may be based on a physician's order if appropriate.

4.3.7 SNACKS AND NUTRITIONAL SUPPLEMENTS

The Contractor shall provide snacks and nutritional supplements as required by SDDC. The cost of the snacks and nutritional supplements will be billed to SDDC at the invoiced cost to the Contractor, excluding overhead and administrative costs.

4.3.8 MENU CYCLE

Meals shall follow a menu cycle pre-approved by the SDDC Administrator or designee with a minimum cycle length of three (3) weeks. Menu cycles shall be changed a minimum of four (4) times per year.

4.3.9 GENERAL CALORIC BASE

The menu at SDDC will have a general caloric base of 2200-2400 calories per day.

4.3.10 THERAPEUTIC DIETS AND SPECIAL CIRCUMSTANCES

Most patients and clients receive regular diets; however, some patients and clients receive therapeutic diets and on occasion SDDC may have a patient who receives tube feedings. The Offeror must demonstrate the ability to meet the therapeutic diet needs and special feeding needs.

A. *SDDC therapeutic diets.* Therapeutic modifications include, but are not limited to:
   1. Low sodium – 3-5 gm and 2 gm
   2. Protein controlled – 60 gm, 50 gm, 40 gm
   3. Low fat/low cholesterol – Step 2
   4. High protein – additional servings of meat/shake supplement/milk
   5. Diabetic
   6. Soft (Mechanical)
   7. Renal

B. *Client therapeutic diets.*
   1. Diabetic Diet (standard 2,200 calories) (doctor can write order for more or less calories)
   2. Heart Healthy (combined this with 2-gram sodium)
   3. Bland
   4. Lactose Intolerance Diet
   5. Medical Vegetarian/Meat Allergy Diet
   6. Gluten Intolerance Diet
   7. Kosher Diet

8. High Fiber Diet (new diet added in replacement of Bran Flakes)
9. Low Potassium Diet (new diet added)

C. The Contractor can expect the following consistency modifications will be needed for some patients and clients:
1. Regular/whole
2. Ground Meat
3. Pureed
4. Soft
5. Thickened Liquids

D. The Contractor should expect the following circumstances for some patients and clients:
1. High fiber – All diets should include 25-35 gm
2. Food allergies
3. Early/late trays
4. Full liquid trays
5. Clear liquid trays
6. Tube feedings
7. Fluid restrictions
8. Six small meals
9. Vegetarian – provide a non-meat substitute (usually peanut butter or cheese)
10. Double portions

4.3.11 MEDICAL DIRECTIVES AND/OR RELIGIOUS REQUIREMENTS

The Contractor will comply with patient dietary requirements that are based on medical directives or religious requirements when a special diet is a basic tenet of a truly held religious belief.

Food substitutions must be available to accommodate food avoidances due to religious beliefs/practices/observances and patient likes/dislikes in compliance with Medicare/Medicaid standards. Vegetarian food substitutions may be needed. Food allergies must also be accommodated and a substitution provided.

The Contractor is liable for any and all expenses related to the physical harm caused to a patient through exposure to a menu item that caused an illness to the patient; e.g. the contractor is liable for the medical bill if a patient was served food that he/she was known to be allergic to and had to be hospitalized or taken to a clinic. Multiple errors in providing special diet meals may result in termination of the contract.

4.3.12 HOLIDAY AND PECIAL MEALS

A minimum of eleven (11) holiday or special meals shall be served each year. Three sample holiday meal menus shall be submitted with the proposal. Holiday meals shall be consistent with traditional meals prepared during each holiday and shall be approved by the SDDC Administrator or designee prior to the menu cycle in which the holiday falls. Additional holiday or special meals may be requested by SDDC and shall be determined by agreement of SDDC and the Contractor. The eleven holiday meals are: New Year's Eve/Day, Martin Luther King Jr. Day, President's Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Indigenous/Columbus Day, Veterans Day, Thanksgiving and Christmas. Holiday and special meals shall be priced at the same amount as regular scheduled meals.

4.3.13 MENU PLANNING

All menus must be approved by the SDDC Administrator or designee prior to implementation. Menus shall be planned in accordance with the National Research Council's Recommended Dietary Allowances (RDA) to meet the nutritional needs of patients and/or clients.

The Dietary Guidelines for Americans 2020-2025 and the USDA MyPlate Guide shall serve as a basis for all menu planning to assure a variety of foods, maintenance or improvement of weight, adequate sources of essential nutrients and fiber, and appropriate amounts of fat, cholesterol, sugar, and salt/sodium. Menus will be endorsed and signed by a Registered Dietician.

The SDDC menu shall be planned with SDDC tested products and recipes for client acceptability. A variety of food flavors, textures, temperatures, and appearances shall be used. The Contractor shall obtain input and approval of menus from the SDDC Administrator or designee.

Approved SDDC menus shall be prepared as approved by SDDC, i.e. if the menu calls for pure ground beef, it must be used unless a dietary substitute is requested or required by a client. The Contractor is responsible for ensuring that the menus for food actually served must be kept on file for 30 days.

The Contractor shall include in the proposal a method to monitor client preferences and to make acceptable adjustments. A sample meal quality assurance assessment form shall be submitted.

Clients can request and receive second helpings unless contraindicated by a prescribed diet. The Contractor will provide an “alternate” menu for all SDDC meals. This is to allow for patient accommodation of meal preference or refusal. Patients wanting a meal from the “alternate” menu shall choose their meal option at least 24 hours prior to the scheduled meal time. Meal choices will be of equal nutritional value for all dietary needs.

The Contractor is required to utilize a menu planning software product that is compatible with the SDDC food service operations to meet the demands of the patients and clients served. The dietary software used by Contractor must have capability of interfacing with SDDC’s electronic health record, MyAvatar by Netsmart. The Contractor will be responsible for the costs to interface with MyAvatar and provide technical project management to work with Netsmart to establish that interface. The interface must be implemented no later than six (6) months after the contract start date.

The menus will be reviewed and approved, in writing, by a Registered Dietitian who is licensed by the State of South Dakota (or independently contracted with the Contractor) to ensure compliance with all the regulations mentioned in this RFP and RDAs for age and gender of all groups.

The SDDS requires milk to be served at two meals (breakfast and lunch) each day for clients under the age of 21 and one meal per day for clients over 21.

4.3.14 NUTRIENT ANALYSIS

A nutrient analysis shall be submitted and maintained to ensure that the RDAs are being met for all patients and clients. Minimum nutrients to be analyzed include protein, vitamin A, vitamin C, iron, calcium, total fat, saturated fat, cholesterol, dietary fiber, and total calories. Analysis of all menu items and foods offered in the menu shall be calculated as a weekly average.

4.3.15 RECIPES AND PRODUCTION

Standardized recipes and portion control shall be submitted and followed for all food preparation
to ensure medical nutrition therapy, nutritional adequacy, and nutrient requirements. All recipes and production directions shall be in writing and followed implicitly to assure consistency of taste and quality in food products served.

Production such as grilling, French frying, steam cooking, etc., of items shall be continuous through each meal period with large quantities prepared as close as possible to the time they will be served, while still maintaining quality and adequate stock to avoid delay in service. The Contractor shall ensure preparation of a sufficient quantity of food to meet the daily population estimates.

The SDDC shall have free access to all records of recipes, production sheets, product specifications, and quantities of food issued.

4.3.16 DOCUMENTATION OF MEALS SERVED

Documentation of all meals served, including substitutions, shall be maintained. A written method for food substitutions shall be maintained and shall be reviewed by a Registered Dietitian who is licensed in South Dakota to assure nutrient content of substituted foods is comparable.

4.3.17 SUPERVISION OF MEAL PREPARATION AND SERVICE

All meal preparation and service shall be supervised by a qualified Food Service Director or designee as described in this RFP to ensure quality, sanitation, texture, consistency, appearance, therapeutic modifications, and temperatures are adequate and maintained throughout preparation, service and delivery of food.

4.3.18 EMPLOYEE AND VISITOR MEALS

The Contractor shall make employee and visitor meals available and must set a cost per meal. The Contractor will be responsible for establishing and maintaining a system for collection of money for employee/visitor meals.

4.3.19 QUALITY ASSURANCE PLAN

The Contractor shall provide a written quality assurance plan that describes the complaint resolution process in place for addressing complaints from clients, and clearly describes how the Contractor will ensure the quality of the products and services being provided. The Contractor will participate in monthly dietary meetings with the SDDC Administrator and other SDDC staff for the purpose of reviewing and addressing compliance and quality issues.

4.4 PROCUREMENT OF FOOD AND DIRECT SUPPLIES

4.4.1 Procurement Practices/Procedures

The Contractor shall maintain strict procurement practices/procedures throughout the entire process of purchasing, receiving, storing, and inventorying food and direct supplies. The Contractor shall pay for all food and direct supplies related to food production, service and management, and bill SDDC as appropriate within the terms of this RFP or future contract.

4.4.2 Minimum Standards for Grades

The Contractor shall demonstrate their ability to purchase food and supplies that conform with the specified minimum U.S. Standards for Grades. In the absence of grade labeling, the Contractor must be able to provide SDDC with packers'

labeling codes or industry accepted grade equivalent standards to verify the minimum grades specified are being used.

For SDDC meals, grade minimum for food items shall be as follows:

A. Meat: USDA No. 1 or choice, cut to IMP specifications. Please note South Dakota forbids the use of any imported beef in State institutions.
B. Seafood: U.S. Grade A, certified.
C. Poultry: U.S. Grade A.
D. Eggs: U.S. Grade A medium size.
E. Pure ground beef: USDA utility or better, not to exceed 18% to 22% fat.
F. Fresh fruits and vegetables: USDA Grade A.
G. Canned fruits, vegetables and juices: USDA Grade A.
H. Frozen fruits, vegetables and juices: USDA Grade A.
I. Dairy products, cheese: USDA Grade A.

These grades are intended as minimum standards only and the Contractor is encouraged to exceed these minimums whenever possible. All other food stuffs not included in the above categories shall be of comparable quality.

Ground beef patties may contain a maximum fat content of the finished raw patty of 18% to 22%. All menu items prefabricated, produced by others or processed by the Contractor containing soy protein derivatives or poultry analogues shall be approved by SDDC prior to service.

4.5 CLEANLINESS, SANITATION AND SAFETY REQUIREMENTS

4.5.1 GENERAL REQUIREMENTS

The Contractor shall show a history of adhering to the highest standards of cleanliness, sanitary and safety practices. The Contractor shall provide required/regular housekeeping, maintenance and sanitation service on the equipment and supplies for all food service equipment and areas. This shall include, but not be limited to, production areas, serving kitchens, refrigerators, freezers, storage areas, and dining and service areas regularly used by food service as well as areas temporarily assigned for food service.

4.5.2 CLEANLINESS REQUIREMENTS

The Contractor is responsible for cleaning of hood ducts, plenums and related vents and fans. The Contractor shall be responsible for routine cleaning and maintenance of hoods and filters. The Contractor may meet the cleanliness requirements using their own staff or may hire an outside vendor to complete the work at their own expense. In the event the contractor does not meet the cleanliness requirements, SDDC reserves the right to use their own staff or hire an outside vendor to complete the work. In this case, the Contractor will reimburse SDDC for the cost of cleaning, whether done by SDDC staff or an outside vendor.

The Contractor shall provide an adequate inventory of table linens, employee uniforms, aprons, jackets, towels, bar swipes, potholders, and such other related food service linens. The Contractor shall be responsible for laundry service, dry cleaning, repairing, and maintaining an adequate inventory of these items. Selection of employee uniforms shall be mutually agreed upon by SDDC and the Contractor.

4.5.3 SANITATION REQUIREMENTS

The Contractor is expected to adhere to applicable state, county and municipal recycling and waste disposal requirements. The Contractor is financially

responsible for the costs to remove garbage from food service and production operations areas and deposit the garbage in exterior dumpsters. SDDC will be financially responsible for the costs of disposing garbage from exterior dumpsters.

The Contractor shall provide waste containers within food service and production areas in sufficient quantity to maintain sanitary standards for garbage disposal. The Contractor shall provide garbage bag liners as needed. Garbage containers shall be kept in a clean and satisfactory condition always and emptied by the Contractor.

4.5.4 SAFETY REQUIREMENTS

With the cooperation of the SDDC, an aggressive program of accident prevention and safety education shall be instituted by the Contractor. Proper instructions and training shall be provided on the use of equipment and techniques of handling food to aid in the goal of having an accident free and safe environment.

Employees are to be trained by the Contractor on where to find safety equipment and how to use such equipment. All injuries and accidents are to be reported to the SDDC the day they occur. SDDC will furnish and maintain fire extinguisher equipment and supplies, including automatic hood extinguisher systems. The Contractor shall be responsible for the costs of First Aid equipment and supplies in all production and food service areas.

The Contractor must provide SDDC one copy of a Material Safety Data Sheet for each item used by the Contractor that is defined as a hazardous material per 29 CFR 1910.1200. The Contractor must still obtain permission from SDDC prior to the use of a hazardous material, including reformulated chemicals.

4.5.5 INSPECTIONS

SDDC retains the right to inspect all manual food areas, dining facilities, storage and auxiliary service rooms and the operation of the Contractor with respect to the quality and quantity of manual food service, the method of service, opening and closing hours, and generally with respect to use, safety, sanitation, and the maintenance of said premises. All areas shall be maintained at a level satisfactory to the SDDC. The SDDC shall have the right to establish reasonable regulations from time to time about such matters and the Contractor agrees to comply with such regulations.

Authorized representatives of the SDDC, or their designees, auditors of the USDA and the Comptroller General of the United States and the SFA’s independent auditors shall have access to all such records for audit and review upon request at a reasonable time and place for making audit, examination, excerpts, and transcriptions. Authorized representatives of the SFA, the SA, or the USDA shall have the right to conduct on-site administrative reviews of the food service program.

Agents of the State Department of Health and other applicable state and federal agencies shall have complete cooperation and access to all food service, production and storage areas and records for inspections that they may conduct. These inspections may be conducted unannounced, at the request of the state or at SDDC's own discretion. The Contractor shall be required to have a Department of Health (DOH) inspection grade higher than 85% or be penalized $500 for each percent below 85%.

A management representative of the Contractor shall conduct equipment and facility maintenance and sanitation inspections periodically, as determined by agreement. Supplier representatives who normally provide equipment and product inspections and reports as part of their services shall be encouraged to perform frequent inspections and shall furnish a copy of each report to the Contractor and SDDC.

The Contractor is responsible to implement corrective operating measures required because of these inspections and report within ten (10) days of notification and by agreement of SDDC to meet or exceed DOH or other regulatory requirements.

4.5.6 FAILURE TO MEET STANDARDS

If the Contractor fails to meet the sanitation standards required by the contract or of any agency having jurisdiction, or fails to comply with the state rules and regulations concerning protection from fire or general safety, SDDC reserves the right to hire outside contractors to perform the necessary work or have the work done by state personnel, and, in either case, charge back the Contractor at actual labor and materials costs plus twenty-five percent (25%) of the labor and materials total cost. SDDC reserves the right to withhold payment for services not rendered by the Contractor as set forth in the contract.

4.6 EQUIPMENT AND SUPPLIES

4.6.1 EQUIPMENT AND SUPPLIES PROVIDED BY SDDC

SDDC shall provide the Contractor with an initial physical inventory of supplies (i.e., hand utensils, cleaning equipment, trays, pans, pots, dishes, glasses, silverware, etc.) and capital equipment at the start of the contract.

SDDC will provide all adaptive equipment needed for patient cares. These include, but are not limited to weighted or molded silverware, red glasses (for contrast with macular degeneration), sectioned plates, and nosey cups. SDDC shall provide the following existing office furniture and equipment for use by the contractor in the performance of the contract at no charge under the same terms applicable to capital equipment contained in the contract: desks, chairs, filing cabinets, and other equipment as negotiated.

Electronic Health Record will be available to approved Contract staff via state approved virtual private network.

With respect to equipment provided by the SDDC, the SDDC makes no implied or express warranties, including but not limited to, the implied warranties of merchantability and fitness for a purpose. However, the Contractor shall have the benefit of any warranty or guarantee given the SDDC by the manufacturer or the seller of the equipment.

Ownership of all non-expendable supplies and capital equipment shall remain with SDDC and shall not be loaned or removed from the grounds without prior written approval. The Contractor shall take such measures as may be reasonably required by the SDDC for the protection against loss by pilferage or destruction.

If food service equipment or other SDDC property is damaged because of negligence or misuse by the Contractor, its employees or agents, including client laborers, and SDDC determines the equipment must be replaced or property

repaired or replaced, the Contractor shall reimburse the SDDC for the full cost of repairs or replacement (including parts and labor).

SDDC is responsible for the repair and replacement of SDDC-owned equipment; however the Contractor is responsible for adequate cleaning and preventative maintenance. SDDC owned food service equipment in need of repair or replacement through normal use shall be brought to the attention of the SDDC Operations Manager who will determine the best course of action for repair or replacement. If the Contractor and/or its staff arrange for repair or replacement of food service equipment owned by SDDC without first consulting SDDC, the Contractor will be responsible for the cost of repair or replacement.

4.6.2 EQUIPMENT AND SUPPLIES PROVIDED BY THE CONTRACTOR

Depletion of supplies shall be replaced to existing standard operational levels by the Contractor at its expense semiannually and on completion or termination of the contract. The specifications for these items shall be arrived at, in writing, by agreement between the Contractor and the SDDC Administrator or designee.

Other equipment not provided by SDDC that the Contractor deems necessary may be provided by the Contractor at its own expense. Installation of such equipment shall require prior approval of the SDDC. The Contractor is solely responsible to make contracts for and payments on all leased rental food services related equipment. The Contractor's purchase of products (food or supplies) which require equipment for their dispensing and have the equipment and service costs prorated in the cost of their product may be purchased for use at the SDDC without prior approval of the SDDC.

The Contractor will provide their own computer equipment and dietary software.

4.7 SPACE USE

4.7.1 CONTRACTOR USE OF FOOD SERVICE AREAS

The Contractor may utilize the space assigned by the SDDC for food service operations. Subsequent modifications of space needs shall be subject to agreement of the SDDC and Contractor.

4.7.2 CONTRACTOR USE OF NON-FOOD SERVICE AREAS

The Contractor cannot use non-food service areas for purposes other than business related to SDDC. When the Contractor uses areas that are not primarily intended for food service (e.g., meeting rooms and lounges) for such purposes as may be required, the Contractor shall be responsible for cleanup which shall involve maintenance and sanitation of the areas, furniture rearrangement and equipment and trash removal.

When the Contractor caters beverages and snacks in a meeting room, the Contractor is responsible for prompt removal of food equipment and food residue from the area following completion of the meeting.

4.8 SECURITY

4.8.1 KEY AND ACCESS CARD CONTROL

The Contractor is responsible for control of keys and access cards obtained from SDDC and the security of those areas used by its representatives. The Contractor will be responsible for the cost for replacement of lost access cards and/or keys and the cost of re-keying and replacement of lock cylinders required because of its negligence and/or loss of keys.

4.8.2 CONTRACTOR SECURITY RESPONSIBILITIES

Designated employees of the Contractor shall be responsible for ensuring all equipment has been turned off, windows closed, lights and fans turned off, and doors locked when not in use.

The Contractor is responsible for the purchase of padlocks and other security devices not currently provided by SDDC that may be required by the Contractor to further ensure revenue, product or property security within the food service areas. The Contractor shall immediately report the facts relating to losses incurred because of theft or break-ins to SDDC Operations Manager.

The Contractor shall follow the SDDC's policies in dealing with improper conduct and shall report all incidences to the SDDC Operations Manager. Emergency calls shall be reported to the SDDC Operations Manager as promptly as possible.

4.8.3 SDDC SECURITY RESPONSIBILITIES

SDDC shall provide the Contractor with safety and security services currently available to food service. If the Contractor requires additional security, it shall be provided by or coordinated through SDDC for which the Contractor agrees to pay prevailing charges.

4.9 UTILITIES/TELEPHONE

4.9.1 GENERAL UTILITY PROVISIONS

SDDC shall provide heat, air conditioning, sewer, electricity, steam, gas, and cold/hot water. The Contractor agrees to exercise care to keep these energy services to a minimum.

SDDC will not guarantee an uninterrupted supply of heat, air conditioning, sewer, electricity, steam, gas, telephone, cold/hot water, or high/low temperature refrigeration. However, SDDC shall use its best efforts to restore services following an interruption. SDDC shall not be liable for any product loss that may result from the interruption or failure of any such utility services or equipment.

Scheduled outages by the SDDC will be coordinated through the SDDC Administrator or designee.

Loss of utility functionality due to the Contractor’s negligence will be the cost responsibility of the Contractor. Repair to systems resulting from Contractor negligence will be the cost responsibility of the future Contractor. This could include loss of utility functionality due to client negligence if the Contractor failed to properly supervise clients.

4.9.2 TELEPHONE SERVICE

SDDC shall provide the Contractor with telephone equipment, installation, and service. SDDC shall determine the style, number, and location of equipment to be provided. The Contractor, at its option, may install additional equipment at its expense.

The Contractor shall have access to local and long-distance service using equipment provided by the SDDC. SDDC shall pay for telephone equipment repair and replacement and line maintenance.

4.10 STATEMENTS, AUDITS, PAYMENTS AND BILLINGS

4.10.1 CONTRACTOR BILLING

SDDC prefers the Contractor submit a weekly invoice by the third working day of the following week. However, the Contractor may submit a monthly invoice to SDDC by the fifth working day of each month covering the preceding month.

The invoice(s) shall include a breakdown of the number of meals served each day for breakfast, lunch and dinner; and shall be further broken out by meals for SDDC clients. The same invoice or an accompanying invoice shall itemize the amount and cost of snacks, nutritional supplements and all other costs associated for meal service at SDDC.~~.~~ A breakdown of types of meals served, number of meals served, special meals, and partial day meals must be included.

Snacks and nutritional supplements must be identified separately and will be billed to SDDC at invoiced cost to the Contractor, excluding overhead and administrative costs.

4.10.2 CRITERIA FOR CONTRACTOR REPORTS

The Contractor's year-to-date reports shall correspond with the State's fiscal year, July 1 through June 30. A month shall be a calendar month. A week shall run from Sunday through Saturday.
Electronic reporting is required. Upon request of SDDC, the Contractor shall meet with SDDC and review each operating statement, explain deviations, discuss problems, and mutually agree on courses of action to improve the results of the required services included in the future contract.

Operating statement adjustments required as a result of review and/or audit shall be identified and reflected on the next period statement.

4.10.3 MAINTENANCE AND SECURITY OF CONTRACTOR RECORDS

The Contractor agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the food service operation, including records and documents regarding the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State.

The Contractor shall retain such records for a period of six (6) years from the close of each fiscal year's operations. If such records are under pending audit, the Contractor agrees to hold such records until such time as the audit is resolved or a longer period upon notification from the SDDC or State.

SDDC, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to food service operations rendered under the contract.

All payments to the Contractor by SDDC are subject to site review and audit as prescribed and carried out by the State. Any over payment of a future contract shall be returned to SDDC/State within thirty (30) days after written notification to the Contractor.

4.10.4 AUDIT REQUIREMENTS

The Contractor agrees to submit to SDDC a copy of an annual entity-wide, independent audit conducted by an independent certified public accounting firm in accordance with Generally Accepted Accounting Principles (GAAP). The audit shall be filed annually with SDDC within a month after completion of the audit.

If federal funds of $500,000 or more have been received by the Contractor, the audit shall be conducted in accordance with OMB Circular A-133 by an auditor approved by the Auditor General to perform the audit. On continuing audit engagements, the South Dakota Auditor General's approval should be obtained annually.

Audits shall be completed and filed with the Department of Legislative Audit by the end of the fourth month following the end of the fiscal year being audited. For an A-133 audit, approval must be obtained by forwarding a copy of the audit engagement letter to:

Department of Legislative Audit
A-133 Coordinator
427 South Chapelle
c/o 500 East Capitol Avenue
Pierre, SD 57501-5070

For either an entity-wide, independent audit or an A-133 audit, the Contractor assures resolution of all interim audit findings. The State's representative or selected auditors may annually, or more often if deemed necessary, examine all financial and operational phases of the Contractor's services.

Periodic reviews, conducted jointly by representatives of the State and the Contractor, shall be made to ensure that the staffing pattern, menu pricing structure and other phases of the operation are conducted in a manner that will provide the best value to the State. The purpose of the review is to ensure that the SDDC is provided with quality, convenient food service, under sanitary and healthful conditions, at the most reasonable prices possible.

The State, to the extent authorized under SDCL Chapter 1-27, will maintain the confidentiality of Contractor's revenue and expense statements, audit and related financial information obtained under this subsection.

4.10.5 PERMITS, LICENSES, BONDS AND TAXES

The Contractor shall be financially responsible for obtaining all required permits, licenses and bonds to comply with pertinent city, county, State and federal laws and regulations. The Contractor shall assume liability for all applicable taxes including, but not limited to, sales, use and property taxes.

5.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

5.1 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.

5.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of 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.

5.3 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.

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.

6.0 PROPOSAL RESPONSE FORMAT

6.1 One original and three hardcopies, and one electronic copy shall be submitted.

6.1.1 The Offeror should provide one (1) copy of their entire proposal, including all attachments, in Microsoft Word AND/OR a PDF (must be in searchable format) electronic format via Secured File Transfer Protocol (SFTP) per the instructions in Section 1.5. Offerors may send the electronically formatted copy of their proposal via email.

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

6.2 All proposals must be organized and tabbed with labels for the following headings:

6.2.1 **RFP Form**. The State's Request for Proposal form (1st page of RFP) completed and signed.

6.2.2 **Executive Summary.** The one-to-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.

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

6.2.3.1 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.

6.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP. The response should identify each requirement being addressed as enumerated in the RFP.

6.2.3.3 A clear description of any options or alternatives proposed.

6.2.4 **Cost Proposal.** Cost will be evaluated independently from 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 8.0 for more information related to the cost proposal.

7.0 PROPOSAL EVALUATION AND AWARD PROCESS

7.1 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:

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

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

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

7.1.4 Proposed project management techniques;

7.1.5 Ability and proven history in handling special project constraints;

7.1.6 Availability to the project locale; and

7.1.7 Familiarity with the project locale.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.5.1 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.

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

7.5.3 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.

8.0 COST PROPOSAL

8.1 PRICING

The Offeror will provide their pricing, which shall consist of their direct and indirect expenses related to providing meals to clients.

8.2 ITEMS/SERVICES OUTSIDE THE NORMAL MEAL SERVICE

For all items/services provided outside the normal meal service, the Offeror will bill SDDC directly. The Offeror will track the costs of such items and will provide reconciliation to SDDC on a quarterly basis.

8.3 ANNUAL PRICING ADJUSTMENT

SDDC will calculate the annual pricing adjustment to the price per meal based upon the following factors:

8.3.1 For the labor related component of the price (hereby assumed to be 60%), the price shall be based upon the wage adjustment recommended by the Governor or approved by the Legislature, whichever is less, for State employees.

8.3.2 For the non-labor component of the price (hereby assumed to be 40%), the price shall be adjusted by the change in the CPI (Consumer Price Index) for the Midwest Urban Food Award From Home series.

8.3.3 Calculation based on the year prior to the year immediately preceding the year of adjustment.

8.3.4 SDDC reserves the right to utilize the 60/40 split identified in A and B above or 3% whichever is less.

Exhibit A
Census by Fiscal Year

FY2021	
JULY 2020	92
AUGUST 2020	87
SEPTEMBER 2020	85
OCTOBER 2020	83
NOVEMBER 2020	83
DECEMBER 2020	83
JANUARY 2021	84
FEBRUARY 2021	84
MARCH 2021	83
APRIL 2021	82
MAY 2021	82
JUNE 2021	79
FY Average	**84**
FY2022	
JULY 2021	78
AUGUST 2021	78
SEPTEMBER 2021	78
OCTOBER 2021	77
NOVEMBER 2021	75
DECEMBER 2021	76
JANUARY 2022	78
FEBRUARY 2022	78
MARCH 2022	78
APRIL 2022	77
MAY 2022	76
JUNE 2022	76
FY Average	**77**
FY2023	
JULY 2022	80
AUGUST 2022	80
SEPTEMBER 2022	79
OCTOBER 2022	78
NOVEMBER 2022	79
DECEMBER 2022	80
JANUARY 2023	81
FEBRUARY 2023	82
MARCH 2023	81
APRIL 2023	83
MAY 2023	81
JUNE 2023	81
FY Average	**80**

CENSUS BASED ON THE COUNT OF THE LAST DAY OF THE MONTH.

Exhibit B

Bureau of Information and Telecommunications
Required IT Contract Terms

Any contract resulting from this RFP will include the State's required IT terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. Due to the changing landscape of IT security and data privacy, the State reserves the right to add additional IT terms and conditions or modify the IT terms and conditions listed below to the resulting contract:

Pursuant to South Dakota Codified Law § 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software, and services; telecommunication equipment, software, and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions, and other units of state government. As part of its duties as the Executive Branch's centralized IT agency, BIT requires the contract terms and conditions of this Exhibit XX. For purposes of this Exhibit, [Vendor Name] will be referred to as the "Vendor."

It is understood and agreed to by all parties that BIT has reviewed and approved only this Exhibit. Due to the ever-changing security and regulatory landscape in IT and data privacy before renewal of this Agreement BIT must review and approve the clauses found in this Exhibit as being the then current version of the clauses and if any additional required clauses are needed. Changes to clauses in this Exhibit must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible.

The Parties agree, when used in this Exhibit, the term "Vendor" will mean the Vendor and the Vendor's employees, subcontractors, agents, assigns, and affiliated entities.

Section I. Confidentiality of Information

For purposes of this paragraph, "State Proprietary Information" will include all information disclosed to the Vendor by the State. The Vendor will 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 Vendor must 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 Vendor 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 Vendor must 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 Vendor agrees to return all information received from the State to the 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 will not include information that:

A. was in the public domain at the time it was disclosed to the Vendor,
B. was known to the Vendor without restriction at the time of disclosure from the State,
C. that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information,
D. was independently developed by the Vendor without the benefit or influence of the State's

information, and

E. becomes known to the Vendor 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. The Vendor understands that this information is confidential and protected under State law. The Parties mutually agree that neither of them nor any subcontractors, agents, assigns, or affiliated entities will 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. The Vendor 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.

Section II. Cyber Liability Insurance

The Vendor will maintain cyber liability insurance with liability limits in the amount of $ _____ to protect any and all State data the Vendor 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 Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this Agreement, then the Vendor will include a requirement for cyber liability insurance as part of the contract between the Vendor 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-party Vendor. The cyber liability insurance will 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 Vendor will 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 Vendor will furnish copies of insurance policies if requested by the State. The insurance will stay in effect for three years after the work covered by this Agreement is completed.

Section III. Rejection or Ejection of Vendor

The State, at its option, may require the vetting of any of the Vendor, and the Vendor's subcontractors, agents, Assigns, or affiliated entities. The Vendor is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor must immediately remove the individual from the project.

Section IV. Software Functionality and Replacement

The software licensed by the Vendor to the State under this Agreement will provide the functionality as described in the software documentation, which the Vendor agrees to provide to the State prior to or upon the execution of this Agreement.

The Vendor agrees that:

A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.
B. If, in the opinion of the State, the Vendor 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 will have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor 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.

Section V. Service Bureau

Consistent with use limitations specified in the Agreement, the State may use the product to provide services to the various branches and constitutional offices of the State of South Dakota as well as county and city governments, tribal governments, and school districts. The State will not be considered a service bureau while providing these services and no additional fees may be charged unless agreed to in writing by the State.

Section VI. Federal Intellectual Property Bankruptcy Protection Act

The Parties agree that the State will be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

Section VII. Non-Disclosure and Separation of Duties

The Vendor will enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State Data or the hardware that State Data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State Data or the hardware the State Data resides on.

Section VIII. Cessation of Business

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any state-owned assets and data. The Vendor will implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

Section IX. Legal Requests for Data

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

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State Data maintained by the Vendor,
B. Consult with the State regarding the Vendor's 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.

Section X. eDiscovery

The Vendor will 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 State Data. The Vendor will 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.

Section XI. Audit Requirements

The Vendor warrants and agrees it is aware of and complies with all audit requirements relating to the classification of State Data the Vendor stores, processes, and accesses. Depending on the data classification, this may require the Vendor to grant physical access to the data hosting facilities to the State or a federal agency. The Vendor will notify the State of any request for physical access to a facility that hosts or processes State Data by any entity other than the State.

Section XII. Annual Risk Assessment

The Vendor will conduct an annual risk assessment or when there has been a significant system change. The Vendor will provide verification to the State's contact upon request that the risk assessment has taken place. At a minimum, the risk assessment will include a review of the:

A. Penetration testing of the Vendor's system;
B. Security policies and procedures;
C. Disaster recovery plan;
D. Business Associate Agreements; and
E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

If the risk assessment provides evidence of deficiencies, a risk management plan will be produced. Upon request by the State, the Vendor will send a summary of the risk management plan to the State's contact. The summary will include completion dates for the risk management plan's milestones. Upon request by the State, the Vendor will send updates on the risk management plan to the State's contact. Compliance with this Section may be met if the Vendor provides proof to the State that the Vendor is FedRAMP Certified and has maintained FedRAMP Certification.

Section XIII. Independent Audit

The Vendor will disclose any independent audits that are performed on any of the Vendor's systems tied to storing, accessing, and processing State Data. This information on an independent audit(s) must be provided to the State in any event, whether the audit or certification process is successfully completed or not. The Vendor will provide a copy of the findings of the audit(s) to the State. Compliance with this Section may be met if the Vendor provides a copy of the Vendor's SOC 2 Type II report to the State upon request.

Section XIV. Service Level Agreements

The Vendor warrants and agrees that the Vendor has provided to the State all Service Level Agreements (SLA) related to the deliverables of the Agreement. The Vendor further warrants that it will provide the deliverables to the State in compliance with the SLAs.

Section XV. Access Attempts

The Vendor will log all access attempts, whether failed or successful, to any system connected to the

hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity. For all systems, the log must include at least: login page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the State, the Vendor agrees to grant the State access to those logs to demonstrate compliance with the terms of this Agreement and all audit requirements related to the hosted system.

Section XVI. Access to State Data

Unless this Agreement is terminated, the State's access to State Data amassed pursuant to this Agreement will not be hindered if there is a:

A. Contract dispute between the parties to this Agreement,
B. There is a billing dispute between the parties to this Agreement, or
C. The Vendor merges with or is acquired by another company.

Section XVII. Password Protection

All aspects of the Vendor's products provided to the State pursuant to this Agreement will be password protected. If the Vendor provides the user with a preset or default password, that password cannot include any 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 defined under federal or state law, rules, or regulations as confidential information or fragment thereof. On an annual basis, the Vendor will document its password policies for all Vendor employees to ensure adequate password protections are in place. The process used to reset a password must include security questions or Multifactor Authentication. Upon request, the Vendor will provide to the State the Vendor's password policies, logs, or administrative settings to demonstrate the password policies are actively enforced.

Section XVIII. Provision of Data

State Data is any data produced or provided by the State as well as any data produced or provided for the State by the Vendor or a third-party.

Upon notice of termination by either party or upon reaching the end of the term of this Agreement, the Vendor will provide the State all current State Data in a non-proprietary format. In addition, the Vendor agrees to extract any information (such as metadata, which includes data structure descriptions, data dictionary, and data) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. If the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Upon the effective date of the termination of this Agreement, the Vendor will again provide the State with all current State Data in a non-proprietary format. In addition, the Vendor will again extract any information (such as metadata) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. As before, if the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Section XIX. Threat Notification

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 any aspect of a system that is holding State Data or a product provided by the Vendor. Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two business days of any such threat. If the State requests, the Vendor will provide the

State with information on the threat.

Section XX. Security Incident Notification for Non-Health Information

The Vendor 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 Policy ("ITSP") attached as BIT Attachment 1. The State requires notification of a Security Incident involving any of the State's sensitive data in the Vendor'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 the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor will 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 Vendor. 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 Vendor 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 Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

A. The Vendor must notify the State contact within 12 hours of the Vendor 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 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 all of the information is not available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.
C. At the State's discretion within 12 hours the Vendor must provide to the State all data available including:

    1. name of and contact information for the Vendor's Point of Contact for the Security Incident,
    2. date and time of the Security Incident,
    3. date and time the Security Incident was discovered,
    4. description of the Security Incident including the data involved, being as specific as possible,
    5. the potential number of records, and if unknown the range of records,
    6. address where the Security Incident occurred, and
    7. the nature of the technologies involved. If not all of the information is available for the notification within the specified time period, the Vendor must provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of 12 hours is acceptable only if it is necessitated by other legal requirements.

D. If the Security Incident falls within the scope of South Dakota Codified Law Chapter 22-40, the Vendor is required to comply with South Dakota law.

The requirements of subsection D of this Section do not replace the requirements of subsections A, B, and C, but are in addition to them.

Section XXI. Handling of Security Incident for Non-Health Information

At the State's discretion, the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

A. fully investigate the incident,
B. cooperate fully with the State's investigation of, analysis of, and response to the incident,
C. make a best effort to implement necessary remedial measures as soon as it is possible, and
D. 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 Vendor and at the Vendor's expense the Vendor 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 Vendor will offer two years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State reserves the right to require the Vendor undergo a risk assessment where the State will determine the methodology and scope of the assessment and who will perform the assessment (a third-party vendor may be used). Any risk assessment required by this Section will be at the Vendor's expense.

If the Vendor 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 12 hours of the investigation report being completed. If the Vendor 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 Vendor 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 Vendor will also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

Section XXII. Security Incidents for 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 Vendor must alert the State contact within 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 Vendor'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 the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State will be required. Probes and scans include, without limitation, pings, and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, if such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Vendor 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 Vendor'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 Vendor is responsible for the Security Incident, and where the State incurs any costs in the investigation, review, or remediation of the Security Incident, the Vendor must 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 Vendor is responsible for the Security Incident, the Vendor must also pay 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 Vendor's services or product(s).

Section XXIII. Adverse Event

The Vendor must notify the State contact within three days if the Vendor 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 Vendor's actions or inactions, the State can require a risk assessment of the Vendor 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 Vendor'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.

Section XXIV. Browser

The system, site, 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, or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

Section XXV. Security Acknowledgment Form

The Vendor will be required to sign the Security Acknowledgement Form which is attached to this Agreement as BIT Attachment 2. 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 Vendor by the State contact before work on the contract may begin. This Security Acknowledgment Form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor, the Vendor's employee(s), and subcontractor's, agents, assigns and affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP). 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 Vendor does not sign another Security Acknowledgement Form covering any employee(s) and any subcontractor's, agent's, assign's, 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 Vendor's, Vendor's employee(s), or subcontractor's, agent's, assign's, 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 Vendor or subcontractors, agents, assigns, or affiliated entities and in accordance with the Vendor's or subcontractor's, agent's, assign's, and affiliated entities' personnel policies. Regardless of the actions taken by the Vendor and subcontractors, agents, assigns, and affiliated entities, the State will retain the right to require at the State's discretion the removal of the employee(s) from the project covered by this Agreement.

Section XXVI. Background Investigations

The State requires any person who writes or modifies State-owned software, alters hardware, configures software of State- owned technology resources, has access to source code or protected Personally Identifiable Information (PII) or other confidential information, or has access to secure areas to undergo fingerprint-based background investigations. These fingerprints will be used to check the criminal history records of both the State of South Dakota and the Federal Bureau of Investigation. These background investigations 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 2-4 weeks to complete this process.

If work assignments change after the initiation of the project covered by this Agreement so that a new person will be writing or modifying State-owned software, altering hardware, configuring software of State-owned technology resources, have access to source code or protected PII or other confidential information, or have access to secure areas, background investigations must be performed on the individual who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any person from performing work under this Agreement whenever the State believes that having the person 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 investigation. The State will provide the Vendor with notice of this determination.

Section XXVII. Information Technology Standards

Any service, software, or hardware provided under this Agreement will comply with State standards which can be found at https://bit.sd.gov/bit?id=bit_standards_overview.

Section XXVIII. Product Usage

The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

Section XXIX. Security

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

By signing this Agreement, the Vendor warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High, Medium, and Low can be described as follows:

   1. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
   2. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
   3. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
   4. **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 Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor 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.

Section XXX. Security Scanning

The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Vendors who do business

with the State must also subscribe to industry security practices and requirements. Vendor s must include costs and time needs in their proposals and project plans to assure they can maintain currency with all security needs throughout the lifecycle of a project. The State will collaborate in good faith with the Vendor to help them understand and support State security requirements during all phases of a project's lifecycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

At the State's discretion, security scanning will be performed and security settings will be put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State's satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Vendor producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

Section XXXI. Malicious Code

A. The Vendor warrants that the Agreement deliverables contain no code that does not support an application requirement.
B. The Vendor warrants that the Agreement deliverables contains no malicious code.
C. The Vendor warrants that the Vendor will not insert into the Agreement deliverables or any media on which the Agreement deliverables is delivered any malicious or intentionally destructive code.
D. In the event any malicious code is discovered in the Agreement deliverables, the Vendor must provide the State at no charge with a copy of or access to the applicable Agreement deliverables that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this Section are in addition to other additional remedies available to the State.

Section XXXII. Denial of Access or Removal of Application or Hardware from Production

During the life of this Agreement the application and 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 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 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 Vendor will be liable for additional work required to rectify issues concerning security, functionality, unsupported third- party technologies, and excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application or hardware. At the discretion of the State, contractual payments may be suspended while the application or hardware is denied access to or removed from production. The reasons can be because of the Vendor'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 Vendor will provide the State with proof of the safety and effectiveness of the remedy, update, or patch proposed before the State provides access to the production system. The State will sign a non-disclosure agreement with the Vendor if revealing the update or patch will put the Vendor's intellectual property at risk. If the remedy, update, or patch the Vendor proposes is unable to present software or hardware that meets the State's requirements, as defined by the State, which may include but is not limited to security, functionality, or unsupported third party technologies, to the State's satisfaction within 30 days of the denial of access to or removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same 30 days then at the State's discretion the Agreement may be terminated.

Section XXXIII. 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 Vendor 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 Vendor.

Section XXXIV. 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 will be the only consideration in licensing compliance related to computing resource capacity.

Section XXXV. Load Balancing

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

Section XXXVI. Backup Copies

The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

Section XXXVII. Payment Card Industry Data Security Standard

Any service provider who possesses or interacts with payment card data must stay current with the Payment Card Industry (PCI) Data Security Standards. The Vendor will enter into a contract with one or more service providers for payment card services under this Agreement. The Vendor will provide to the State a written acknowledgement from any such service provider with whom the Vendor contracts for such services under this Agreement which acknowledgement will state that the service provider is committed to maintaining proper security of the payment card data in its possession and is responsible for the security of payment card data the service provider possesses or otherwise stores, processes, or

transmits on behalf of the Vendor. The Vendor must ensure that the service provider(s) used by the Vendor meet the Payment Card Industry Data Security Standards. The Vendor will annually review the service provider(s) policies and procedures and supporting documentation. The State at its discretion, can require the Vendor to provide the State with an annual report on the status of compliance of their service provider(s) with the Payment Card Industry Data Security Standards.

Section XXXVIII. Payment Card Industry Data Security Standard

The service provider must stay current with the Payment Card Industry (PCI) Data Security Standards. The State requires an acknowledgement from all service providers who possess or interact with payment card holder data that the service provider is committed to maintaining proper security of the payment card holder data in their possession and is responsible for the security of payment card data the service providers possess or otherwise store, process, or transmit on behalf of the State. To assure continued compliance with the current Payment Card Industry Data Security Standard, the State requires that the service provider acknowledge its understanding and acceptance of this requirement and provide an annual report on the service provider's Payment Card Industry Data Security Standard compliance status.

Section XXXIX. Payment Card Industry Qualification Requirements for Qualified Integrators and Resellers

When having a payment card application implemented, configured, or supported the Vendor and any subcontractor used by the Vendor to fulfil the terms of this Agreement will have successfully met the Payment Card Industry qualification requirements for Qualified Integrators and Resellers (QIR). Should the Vendor or any subcontractor(s) used by the Vendor have their QIR revoked or fail to maintain their QIR the Vendor must immediately cease trying to implement, configuring and or supporting payment card application(s) required by the terms of this Agreement and inform the State Contact. At the State's discretion the Agreement may be terminated without any further obligation of the State.

Section XL. Use of Abstraction Technologies

The Vendor's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Vendor warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Vendor and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Vendor will correct the problem at no additional cost.

Section XLI. Scope of Use

A. There will be no limit on the number of locations, or size of processors on which the State can operate the software.
B. There will be no limit on the type or version of operating systems upon which the software may be used.

Section XLII. License Agreements

The Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements (EULAs), 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, EULAs, and terms of use will be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users will 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 will control and supersede the language of any such agreements to the contrary.

Section XLIII. Web and Mobile Applications

A. The Vendor's application is required to:

1. 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,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. 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,
7. 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,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. 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),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,
11. access no data outside what is defined in the "About" information for the Vendor's application,
12. conform to Web Content Accessibility Guidelines 2.0,
13. have Single Sign On capabilities with the State's identity provider,
14. have an opening screen that states, in an easy-to-read font, that the application is gathering or accessing health or medical information and the user's privacy is not protected by federal regulations if any health or medical information is gathered or accessed by the application that is not protected by HIPAA and HITECH rules and regulations, and
15. any application to be used on a mobile device must be password protected.

B. The Vendor is required to disclose all:

1. functionality,
2. device and functional dependencies,
3. third party libraries used,
4. methods user data is being stored, processed, or transmitted,
5. methods used to notify the user how their data is being stored, processed, or transmitted,
6. positive actions required by the user to give permission for their data to be stored, processed and or transmitted,
7. methods used to record the user's response(s) to the notification that their data is being stored, processed, or transmitted,
8. methods used to secure the data in storage, processing, or transmission,

9. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits,
10. methods used to create and customize existing reports,
11. methods used to integrate with external data sources,
12. methods used if integrates with public cloud provider,
13. methods and techniques used and the security features that protect data, if a public cloud provider is used, and
14. formats the data and information uses.

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

Section XLIV. Intended Data Access Methods

The Vendor's application will not allow a user, external to the State's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Vendor's application can only access data by methods consistent with the intended business functions.

If the State can demonstrate the application flaw, to the State's satisfaction, then the Vendor will rectify the issue, to the State's satisfaction, at no cost to the State.

Section XLV. Application Programming Interface

Vendor documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Vendor's application programming interface and tutorials. The tutorials must include working sample code.

Section XLVI. Access to Source and Object Code

The Vendor will provide access to source and object code for all outward facing areas of the system where information is presented, shared, or received whether via browser-based access and programmatic-based access including but not limited to application program interfaces (APIs) or any other access or entry point accessible via the world wide web, modem, or other digital process that is connected to a digital network, radio-based or phone system.

Section XLVII. Data Location and Offshore Services

The Vendor must provide its services to the State as well as storage of State Data solely from data centers located in the continental United States. The Vendor 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 prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

Section XLVIII. Vendor Training Requirements

The Vendor, Vendor's employee(s), and Vendor'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:

A. legal requirements for handling data,
B. media sanitation,
C. strong password protection,
D. 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,
E. security incident response, and

F. Protected Health Information.

Section XLIX. Internet of Things (IoT)

The IoT device(s) provided to the State by the Vendor pursuant to this Agreement must have the most current security patches and software/firmware upgrades available. As part of the pre-installation process the Vendor must inform the State on how the Vendor will ensure that the patches and upgrades for the IoT device(s) are kept current and the State must approve the proposed process. Any default passwords must be removed from the IoT device(s) before or during installation. There must be no means of accessing the device's embedded computer system that bypasses security mechanisms, for example methods commonly referred to as "backdoors". The State must be informed of all components used to connect to the IoT device(s) and where and how any data it gathers will be stored. The State must be informed of all entities or systems that the IoT device(s) will transmit data to or receive any data from. The State must be notified of any patches or upgrades to be made prior to the installation of those patches or upgrades and given sufficient time to do a security scan of those patches and upgrades before installation. The State may remove from the State's network any IoT device found to pose a security risk and the Vendor must remedy the impact to the State for the IoT device removal.

Section L. Data Sanitization

At the end of the project covered by this Agreement the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities will return the State Data 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 Vendor 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 Vendor will use a process and procedure that does satisfy the State.

This contract clause remains in effect for as long as the Vendor, and Vendor's subcontractors, agents, assigns, and affiliated entities have the State data, even after the Agreement is terminated or the project is completed.

Section LI. Banned Hardware and Software

The Vendor will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Vendor will immediately notify the State if the Vendor becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

Section LII. Hardware Passwords

Any hardware installed on the State network must have any default passwords changed when the hardware is configured to meet State password requirements in the Information Technology Security Policy, see BIT Attachment 1.

Section LIII. Use of Portable Devices

The Vendor must 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 Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

Section LIV. Remote Access

The Vendor will 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 legal requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication. If the State Data that is being remotely accessed is legally protected data or considered sensitive by the State, then:

A. The device used must be password protected,
B. The data is not put onto mobile media (such as flash drives),
C. No non-electronic copies are made of the data, and
D. A log must be maintained by the Vendor detailing the data, which was accessed, when it was accessed, and by whom it was accessed.

The Vendor must follow the State's data sanitization standards, as outlined in this Agreement's Data Sanitization clause, when the remotely accessed data is no longer needed on the device used to access the data.

Section LV. Data Encryption

If State Data will be remotely accessed or stored outside the State's IT infrastructure, the Vendor warrants that the data will be encrypted in transit (including via any web interface) and at rest at no less than AES256 level of encryption with at least SHA256 hashing.

Section LVI. Rights, Use, and License of and to State Data

The parties agree that all rights, including all intellectual property rights, in and to State Data will remain the exclusive property of the State. The State grants the Vendor a limited, nonexclusive license to use the State Data solely for the purpose of performing its obligations under this Agreement. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

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

A. The Vendor will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, use, 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 applicable federal, state, or international law, rule, regulation, or ordinance. Such security measures will be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
B. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.
C. The Vendor will not use State Data for the Vendor's own benefit and will not engage in data mining of State 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.

Section LVII. Third Party Hosting

If the Vendor has the State's data hosted by another party, the Vendor must provide the State the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the State's data will always reside in the continental United States 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 Vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with 180 days' advance notice of this change and at that time provide the State with the information required above.

Section LVIII. Securing of Data

All facilities used to store and process State 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 Vendor'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.

Section LIX. Security Processes

The Vendor will 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 Vendor. For example: virus checking and port sniffing.

Section LX. Import and Export of Data

The State will have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other vendors.

Section LXI. Audit Authorization

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

The Vendor agrees to work with the State to rectify any serious security issues revealed by the security audit or security scanning. This includes additional security audits and security scanning that must be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Vendor 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. It is required that any security audits must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) irrespective of there being any PCI DSS data involved.

Section LXII. System Upgrades

The Vendor must provide advance notice of 30 days to the State of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software, or firmware with a newer or improved version, in order

to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scans can include penetration testing of a test system at the State's discretion.

Section LXIII. Use of Production Data in a Non-Production Environment

The Vendor cannot use protected State Data, whether legally protected or protected by industry standards, in a non- production environment. Any non-production environment that is found to have legally protected production data, must be purged immediately and the State contact notified. The State will decide if this event is to be considered a security incident. "Legally protected production data" is any data protected under federal or state statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated, or hashed is no longer considered to be legally protected.

Section LXIV. Banned Services

The Vendor 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.

Section LXV. Multifactor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor's subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 2 Authentication Assurance for MFA* as defined in NIST 800-63.

Exhibit C
Security and Vendor Questions

Basic Vendor Information

Vendor Legal Name:

Vendor Address:

Directions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. The Bureau of Information and Telecommunications (BIT) recommends that you utilize your BIT Point of Contact (POC) to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards of the state.

If you do not know the details of the technologies the vendor will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Vendors: The following questions help the State determine the best way to assess and integrate your product or service technology with the State's technology infrastructure. Your response to the questions allows BIT an opportunity to review the security of your product, and helps BIT make an informed decision and recommendation regarding your technology or service. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

The State understands that some of the information you may provide when answering the questions is considered confidential or proprietary. Please mark which answers you deem to be confidential/proprietary information. Access to this confidential information will be limited to those state employees who have a need to know. In addition, the State will maintain the confidentiality of the marked information, and the marked information may be exempt from disclosure to the public per the State's Open Records Laws.

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contact.

System/Product: The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.			
Response			
#	BIT	Question	Select all that apply

1	DC DEV	Is your proposed solution a cloud-based solution or an on-prem solution?	State Hosted On-prem (dedicated VM/infrastructure) State Cloud Provider (PaaS Solution) Vendor Hosted Other: (Please state)

2	DC DEV TEL	What type of access is required by vendor or proposed solution to state hosted or external resources?	☐ Not Required ☐ VPN ☐ API ☐ SFTP ☐ Other: (Please state)
3	DC	What type of access is required by vendor to maintain and support the solution?	☐ Not Required ☐ Citrix (For On-prem) ☐ State Cloud Access ☐ Other: (Please state)
4	TEL	If an on-prem solution, which of the following will apply?	☐ IoT Hardware ☐ Non-Windows or non-domain joined solution. ☐ Windows-based domain joined hardware. ☐ Other: (Please state)
5	DC TEL	Does your proposed solution include/require additional devices connected to the application for activities such as scanning or printing?	☐ Yes ☐ No
6	DC	Does the proposed solution include the use of email?	☐ Yes ☐ No If “Yes”, please describe how email will be used:
7	POC TEL	Will there be any desktop software installs, policies, or software required on state managed computers as part of this product?	☐ Yes ☐ No If “Yes”, please define:
8	POC	If there are desktop software installs, please provide a link to the licensing requirements or a copy of the licensing requirements.	Please provide link below, if applicable:
9	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	☐ Yes ☐ No If “Yes”, please define:
10	POC	Will any browser plugins be required to install, access, or use this product?	☐ Yes ☐ No If “Yes”, please define:
11	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	☐ Yes ☐ No If “Yes”, please define:

12	POC	Will any Bluetooth or RF frequency devices be required as part of this product or project?	☐ Yes ☐ No If “Yes”, please define:
13	POC	What operating system is the software/hardware compatible with?	☐ Microsoft Windows 10 ☐ Microsoft Windows 11 ☐ Other (please specify): ☐ Not Applicable
14	POC	For Vendor Hosted solutions, where are your data centers located (Please include locations for disaster recovery)?	Please provide locations:

Section A. System Security The following questions are relevant for all vendors or third parties engaged in this hardware, application, or service and pertain to relevant security practices and procedures.						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed
A1	DC x	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on? Please explain the authentication protocol(s) available to meet the State’s single sign-on requirements and how that is implemented with one or more identity providers.				
A2	DC TEL x	Will the system provide internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				
A3	POC	Will the system have role-based access?				
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, multi-factor authentication)? Which mitigations are in place? What are the optional mitigations?				
A5	DC TEL	Are account credentials hashed and encrypted when stored? If “Yes” please describe the encryption used (e.g. SHA256).				

A6	DC TEL x	The protection of the State's system and data is of upmost importance. Web Application Vulnerability Scans must be done if: • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. The State would want to scan a test system; not a production system and will not do penetration testing. The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Will you allow the State to scan a test system? If no, please explain or provide an alternative option to ensure protection of the State's system and data.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				

A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there any additional components or configurations required outside of the base product to meet the State's security needs?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				

A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-3, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				

A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based? If required, would you be willing to undergo fingerprint-based background checks?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				

		d. Physical access to your data center(s)				
		e. Code changes				
		f. Other:				
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?				

A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device, personal device(s), or other non-company owned system(s)?				
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				
A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				

		b. Is the audit performed annually?				
		c. When was the last audit performed?				
		d. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		e. If it is a SOC 2 audit report, what level is it?				
		f. Does the audit include cloud service providers?				
		g. Has the auditor always been able to attest to an acceptable audit result?				
		h. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or HITRUST?				

A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC TEL	(Only to be used when medical devices are being acquired.) Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the federal government's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B. Hosting

The following questions are relevant to any hosted applications, systems, databases, services, and any other technology. The responses should not assume a specific hosting platform, technology, or service but instead the response should address any hosting options available for the proposed solution.

For state-hosted systems that reside in a state-managed cloud:

To minimize impacts to project schedules, vendors are required to provide architectural plans, resource needs, permission plans, and all interfaces – both internal to the state and internet facing for cloud hosted systems. The documentation provided will be reviewed as part of the initial assessment process. If selected for award of a contract, and once the state has approved the submitted materials, a test environment will be provided after contract signature. Systems will be reviewed again before being moved to a production environment. Any usage or processes that are deemed out of compliance with what was approved or represent excessive consumption or risk will require remediation before being moved to production.

Response

#	BIT	Question	YES	NO	NA	Explain answer as needed
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?				
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: • Security for their I/T systems; • Staff vetting; • Staff security training?				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				

B10	DC	How do you secure Internet of Things (IoT) devices on your network?				
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B15	TEL	How do you monitor your application, systems, and data center for security events, incidents, or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC TEL	What anti-malware product(s) do you use?				
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				
B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database The following questions are relevant to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed
C1	DC	Will the system require a database?				
C2	DC	If a Database is required, what technology will be used (i.e. Microsoft SQL Server, Oracle, MySQL)?				
C3	DC	If a SQL Database is required does the cost of the software include the cost of licensing the SQL Server?				
C4	POC	Will the system data be exportable by the user to tools like Excel or Access at all points during the workflow?				
C5	DC DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C6	DC DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Contractor Process The following questions are relevant for all vendors or third parties engaged in providing this hardware, application, or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed
D1	DC POC	Will the vendor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D5	TEL	What release criteria does your company have for its products regarding security?				
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software				
		b. Does it outline and establish a consistent and predictable support timeline?				
D8	DC	How are patches, updates, and service packs communicated and distributed to the State?				
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a. Can patches and service packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or service pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?				
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?				
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code, or unintended, "dead," or malicious code? What tools are used?				

D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?				
D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?				
D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?				
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?				
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.				

D30	DC	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				
D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the acquirer from these issues in the license agreement? Provide a brief explanation.				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of “trigger” events.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State’s discretion, a contractor’s answers to the follow up questions may be required in writing and/or verbally. The				

		answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development The following questions are relevant to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor.						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed.
E1	DEV POC x	What are the development technologies used for this system?				If marked yes, indicate version.
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If yes, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				

E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				
		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these products?				
E20	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.				
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device, what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open-source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open Web Application Security Project (OWASP) Top Ten?				

F. Infrastructure The following questions are relevant to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system, the questions can be marked "NA".						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed.
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F4	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F5	DC x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F6	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F7	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F9	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F10	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.).				

		Would this affect the implementation of the system? If yes, explain.				

F12	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F13	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at: https://bit.sd.gov/bit?id=bit_standards_overview .				
F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				
F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F20	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				

		g. MS Windows Updates				
		h. Windows Defender				
F21	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS, and desktop security infrastructure. Would this affect the implementation of the system?				

F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process The following questions pertain to how your business model interacts with the State's policies, procedures, and practices. If the vendor is hosting the application or providing cloud services, questions dealing with installation or support of applications on the State's system can be marked "NA".						
Response						
#	BIT	Question	YES	NO	NA	Explain answer as needed.
G1	DC	a. If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?				
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.				
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.				
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?				
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).				

G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer- based training, online educational forums, or sponsor conferences related to the software?				
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?				
G15	DC	Are any of the professional services you plan to provide located outside the United States (e.g., help desk or transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POC x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party, or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				