STATE OF SOUTH DAKOTA
DEPARTMENT OF HEALTH AND DEPARMENT OF REVENUE
455 E CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501

REQUEST FOR PROPOSAL TO DEVELOP AND IMPLEMENT THE SOUTH DAKOTA MEDICAL MARIJUANA PATIENT REGISTRY, VERIFICATION, AND BUSINESS LICENSING SYSTEM

PROPOSALS ARE DUE NO LATER THAN 5:00 PM CDT JUNE 11, 2021

RFP # 2357 BUYER: Sakura Rohleder EMAIL: Sakura.Rohleder@state.sd.us

READ CAREFULLY

FIRM NAME: AUTHORIZED SIGNATURE:

ADDRESS: TYPE OR PRINT NAME:

CITY/STATE: TELEPHONE NO:

ZIP (9 DIGITS): FAX NO:

E-MAIL:

PRIMARY CONTACT INFORMATION

CONTACT NAME: TELEPHONE NO:

FAX NO: E-MAIL:

Table of Contents

1. GENERAL INFORMATION

1.1 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard I/T contract terms listed in Appendix C, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix A may be altered or deleted.
The offeror must state if there are any issues with the contract terms in Appendix C. The issues should be fully described along with any proposed changes. If the offeror does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the offeror. There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix D that 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.

1.2 BACKGROUND INFORMATION FOR THE RFP

In 2020, South Dakota voters passed Initiated Measure 26, now codified in the South Dakota Codified Laws as SDCL Ch. 34-20G, which legalizes the medical use of marijuana effective on July 1, 2021. The initiated measure directs the South Dakota Department of Health (DOH) to create a medical cannabis program and provides the necessary authority to promulgate rules related to that program. The measure contains a caregiver provision that allows a designated caregiver to cultivate or purchase cannabis on behalf of a qualifying patient and establishes various medical marijuana establishments. This measure requires qualifying patients, designated caregivers, and those who wish to operate medical marijuana establishments to be registered with the state, and the state has the responsibility to approve, deny, or revoke both patient cards and licenses.
The measure imposes multiple statutory deadlines that the state must meet:

- the secure web-based patient verification system must be in place by October 29, 2021;
- the department shall issue registry identification cards by November 18, 2021; and
- the department must promulgate rules by October 29th, 2021

Thus, it is pivotal that the appropriate systems are implemented in a timely fashion to meet the statutory deadlines.

South Dakota voters also passed Constitutional Amendment A in 2020, which legalizes the recreational use of marijuana. Although 6th Judicial Circuit Court held the amendment unconstitutional, the matter is under appeal and the South Dakota Supreme Court is set to hear oral arguments on April 28, 2021. The parties have asked the court to consider the proceedings on an expedited schedule. The provisions of Amendment A direct the South Dakota Department of Revenue (DOR) to implement a recreational marijuana program,

regulate the recreational marijuana market, and collect an excise tax on the retail sale of marijuana. Because of the potential that the South Dakota DOR will need to implement the provisions of Amendment A at the same time that the South Dakota DOH will be implementing SDCL 34-20G, this request for proposal is a joint proposal issued by both DOH and DOR. The DOH will be the owner of all three systems being solicited in this proposal; however, pending the outcome of the Amendment A litigation, other state agencies including DOR may also use these same solutions.

1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The South Dakota Department of Health is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Health. The reference number for the transaction is RFP# 2357. This number must be referred to on all proposals, correspondence, and documentation relating to this RFP.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	April 26, 2021
Deadline for Submission of Emailed Inquiries	May 18, 2021
Deadline for Responses to Emailed Inquiries	May 28, 2021
Proposal Submission	June 11, 2021
Oral Presentations/discussions (if required)	July 2021
Anticipated Award Decision/Contract Negotiation	August 27, 2021
Anticipated Contract Start Date	September 2021

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the DOR by the date and time indicated in the Schedule of Activities. Proposals received after the deadline will be late and ineligible for consideration. Offerors must submit 1 original, 1 electronic copy, and 1 electronic copy with propriety information redacted.

Cost will be evaluated as part of the technical proposal. Offerors may submit multiple costs in their proposal. All costs related to the provision of the required service must be clearly stated and included in each proposal offered.

All proposals must be originals signed by an agent of the offeror that is legally authorized to bind the offeror to the proposal. Proposals that are not properly signed may be rejected. The proposals must be submitted in a sealed envelope, marked with the appropriate RFP Number and Title. The words "Sealed Proposal Enclosed" must be prominently denoted on the outside of the shipping container.
Proposals must be addressed and labeled as follows:

REQUEST FOR PROPOSAL # 2357
DUE: JUNE 11, 2021
BUYER: SAKURA ROHLEDER

SOUTH DAKOTA DEPARTMENT OF REVENUE
445 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501

No proposal shall be accepted from 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 offeror shall attach an explanation to the offer.

1.7 NON-DISCRIMINATION STATEMENT

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

1.8 RESTRICTION OF BOYCOTT OF ISRAEL

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

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

1.9 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.

1.10 OFFEROR INQUIRIES

All written questions should be sent to Sakura Rohleder, at Sakura.Rohleder@state.sd.us . Only emailed questions will be accepted.

Offerors and their agents may submit questions concerning this RFP to obtain clarification of requirements via email ONLY. No questions will be accepted after the date and time indicated in the above schedule of activities. Questions must be directed to Sakura Rohleder, at Sakura.Rohleder@state.sd.us, with the subject line "RFP 2357". The questions and their answers will be sent to all offerors that submitted questions or requested the questions and answers via email before the proposal submittal date and will be sent by the date and time indicated in the above calendar of events.

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.

1.11 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.

1.12 LENGTH OF CONTRACT

The estimated length of the contract is 5 years with the possibility of option to extend the contract period by additional 3 years. The first year will include programming and implementation of software, and the remaining 4 years will address maintenance, training, and technical support.

1.13 PRESENTATIONS/DEMONSTRATIONS

Presentations and demonstrations will be scheduled after the submission of proposals and will be made at the offeror's expense. Demonstrations must follow the Use Cases under Appendix A, and each vendor is solely responsible for demonstrating appropriate use cases based on their proposal.

1.14 DISCUSSIONS

At the State's discretion, the offeror may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the offeror's expense.

1.15 NEGOTIATIONS

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 component 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.

1.16 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. The laws of South Dakota shall govern this transaction.

2. STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as listed below, along with any additional terms and conditions as 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 start on _____and end on ____unless terminated sooner pursuant to the terms hereof.

2.3 The Contractor will not 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 TOTAL CONTRACT AMOUNT is an amount not to exceed $_____. 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 chapter 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 million 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 million.

C. Business Automobile Liability Insurance:
The Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than $1 million 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 180 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 affected 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 venue 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_____, 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.

3. SCOPE OF WORK

The scope of this RFP is to solicit the Modifiable Off-The-Shelf Software (MOTS) or multiple software that provide patient registry, verification, and business application licensing for South Dakota Medical Marijuana Program.

Interested vendors must submit a proposal that satisfies all three components of this RFP.
A proposal must clearly separate details of the functionality and the cost breakdown for each of the component. Additionally, if any of the components fail to meet the technical, security, support and maintenance, or communication requirements in this RFP, it must be clearly stated in the proposal.

Furthermore, all interested vendors must submit an integration plan between the proposed solution and seed-to-sale tracking systems, including the list of seed-to-sale tracking systems that the proposed solution has successfully integrated in the past. Currently, the State does not have any seed-to-sale tracking system, and this RFP does not include solicitation for any seed-to-sale tracking system. However, the State may implement a tracking system in the future, therefore , the successful integration of proposed solutions with seed-to-sale tracking system and a thorough integration plan will be part of the selection criteria.

3.1 SOFTWARE REQUIREMENTS

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE IN THE PROPOSAL
3.1a	Individual Account	The registry must allow qualifying patient or caregiver to create an account to apply for the identification card for notification purposes.		
3.1b	Patient Application	The registry must allow qualifying patient or qualifying patient's power of attorney to submit an application for patient registration via this portal. The application must include the following: • The name, address, and the date of birth of the qualifying patient unless the patient is homeless; • The name, address, and telephone number of the qualifying patient's practitioner; • The name, address, and the date of birth of the designated caregiver or designated caregivers; • If the qualifying patient designates a designated caregiver, a designation as to whether the qualifying patient or the designated caregiver will be allowed to possess and cultivate cannabis plants for the qualifying patient's medical use; • The name of no more than two dispensaries that the qualifying patient designates if any; • Whether the person submitting the application is a qualifying patient or his/her power of attorney: • Whether or not the qualifying patient is a resident or non-resident of South Dakota; • Terms and Condition agreement checkbox; and • Additional information required by the rules promulgated by DOH The registry must provide the copy of the completed application to the applicant.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1c	Attach Required Documents for Patient Registry	The registry must require the following documents as part of application: • A written certification issued by a practitioner within 90 days immediately after the date of an application; • If more than one designated caregiver is designated at any given time, documentation demonstrating that a greater number of designated caregiver are needed due to the patient's age or medical conditions; and • If patient's power of attorney is submitting the application on behalf of the patient, the supporting document must be submitted. The registry must flag application from a qualifying patient who is younger than 18 years of age unless he/she submits the following documentation; and • Written explanation from the qualifying patient's practitioner about the potential risk and benefits of the medical use of cannabis to the custodial parent or legal guardian with responsibility for health care decision for the qualifying patient. Optional: Vendors may propose a model where practitioner directly uploads the written certification and recommendation to the system as an alternative document approval process.		
3.1d	Data Validation	The registry must have data validation function to prevent missing data or data type errors		
3.1e	Patient Fee Collection	Qualifying patient must pay a fee through this portal. The registry must allow payment via cash or check.		
3.1f	Caregiver Application	The registry must allow caregiver to submit an application for patient registration via this portal. Caregiver must meet all of the criteria: • Is at least 21 years old; • Has agreed to assist with a qualifying patient's medical use of cannabis; • Has not been convicted of a disqualifying felony offence; and • Assists no more than 5 qualifying patients with the medical use of cannabis, unless the designated caregiver's qualifying patients each reside in on are admitted to a health care facility or residential care facility where the designated caregiver is employed If an applicant fails to meet any of these criteria, it should be flagged for DOH staff for review. Application must include the following fields: • The name, address, and the date of birth of the qualifying		

		patient unless the patient is homeless; • The name, address, and the date of birth of the designated caregiver or designated caregivers; • Additional information required by the rules promulgated by DOH The registry must provide the copy of the completed application to the applicant.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1g	Attach Required Documents for Caregiver Registry	The registry must require the following documents as part of application: • Documents required by the rules promulgated by DOH If the designated caregiver is applying to be the caregiver for a minor, a written consent from the custodial parent or legal guardian with responsibility for the health care decisions for the qualifying patient allowing the qualifying patient's medical use of cannabis, consent to serve as patient's designated caregiver, and consent to control the acquisition of cannabis, dosage, and the frequency of the medical use of cannabis by qualifying patient must be submitted as part of the application.		
3.1h	Caregiver Fee Collection	Caregiver must pay a fee through this portal. The registry must allow payment via cash or check.		
3.1i	Patient Medical Marijuana Card Issuance	The registry must issue an identification card containing the following information: 1. The name of the cardholder; 2. A designation of whether the cardholder is a qualifying patient or a designated caregiver; 3. The date of issuance and expiration date of the registry identification card; 4. A random 10 digit alphanumeric identification number, containing at least 4 number and at least 4 letters, that is unique to the cardholder 5.A clear indication of whether the cardholder has been designated to cultivate cannabis plants for the qualifying patient's medical use; 6. A photograph of the cardholder; and 7. The phone number or website address where the card can be verified. The vendor should specify the preferred printing software, machine model, and the associated cost in the proposal if they have specific integration requirements. The vendor may also propose an option to work with a third-party vendor for card printing as an alternative method.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1j	Caregiver Medical Marijuana Card Issuance	The registry must issue an identification card containing the following information: 1. The name of the cardholder; 2. A designation of whether the cardholder is a qualifying patient or a designated caregiver; 3. The date of issuance and expiration date of the registry identification card; 4. A random 10-digit alphanumeric identification number, containing at least 4 number and at least 4 letters, that is unique to the cardholder 5. If the cardholder is a designated caregiver, the identification number of the qualifying patient the designated caregiver will assist must be displayed on the card; 6. A clear indication of whether the cardholder has been designated to cultivate cannabis plants for the qualifying patient's medical use; 7. A photograph of the cardholder; and 8. The phone number or website address where the card can be verified. The vendor should specify the preferred printing software, machine model, and the associated cost in the proposal if they have specific integration requirements. The vendor may also propose an option to work with a third-party vendor for card printing as an alternative method.		
3.1k	Patient/Caregiver Dashboard	Provide a dashboard where patients/caregivers can see the status of their application.		
3.1l	Patient/Caregiver Communication	Provide a communication feature to send automatic notification and alerts to patients/caregivers. The registry must provide a communication feature where DOH staff can directly communicate with specific applicants in a secure manner. The record of communication between the DOH personnel and applicant or cardholder be stored and reviewable in the system. The communication record should include sender, recipient, date and time of communication, and the content of the communication.		
3.1m	Patient/Caregiver Letter Generation	The registry system should have a letter generating component where DOH personnel can quickly customize patient communication letters based on multiple routine scenarios or communication needs. The template letters include, but not limited to the following:		

		• Renewal • Incomplete Application		
PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1n	Department Review of Applications	Allow DOH personnel to review, accept, or deny the applications. DOH personnel may deny an application or renewal of qualifying patient's registry identification if the applicant: • Does not provide the required information, fee, or materials; • Previously had a registry identification card revoked; or • Provided false information Additionally, caregiver application can be denied by DOH staff for the following reasons: • The applicant does not provide the information required: • The designated caregiver previously had a registry identification card revoked: or • The applicant or the designated caregiver provide false information The registry must create and provide a written notice to the qualifying patient of the reason for denying a registry identification card to the qualifying patient or the designated caregiver.		
3.1o	Internal Edits	DOH staff should have ability to edit application records. The edit capability should be provided to certain personnel based on their security role in the registry system to maintain adequate internal control and data integrity.		
3.1p	Internal Dashboard	Provide a dashboard where DOH staff can see the list of application to be reviewed. The dashboard should provide sort and filter feature where DOH staff can organize the applications.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1q	Internal Workflow	The registry should have ability to automatically move applications through the process set by DOH from application submission to the card issuance. The portal should automatically assign applications to appropriate DOH personnel based on role set in the system with ability to manually select applications for review or approval. Additionally, the workflow should include violation queue where all the submitted applications with missing documents or missing information fields are routed to streamline the workflow process to ultimately yield completed applications. DOH personnel should receive alerts or notification when applications are assigned to them.		
3.1r	Data Import and Export	Export data in the system in CSV or Excel format. The registry must provide the ability to create custom reports based on selected fields, and the ability to save certain reports to reduce redundancies. DOH staff must have the ability to import data to registry in case they receive paper applications via e-mail or mail.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1s	Registry Reporting	The registry must have reporting functionality with easy-to-use query function. The registry must have reporting tool with sort and filter function, an ability to save and share custom report specification, and an ability to export the report in various formatting including Microsoft Excel or PDF. The registry should also come with templates of reports including but not limit to the following list: • Total number of application received for medical marijuana patient or caregiver cards • Total number of approved application for medical marijuana patient or caregiver cards • The number of revocations, suspensions, and non -renewals • The percentage breakdown of qualifying conditions • Total fees collected for medical marijuana patient or caregiver cards by payment type • Total number of physicians providing written recommendations for medical marijuana • Total number of medical marijuana patients approved by physicians The template reports should contain the latest data at the time of export, with the ability to set the date range for the reports.		
3.1t	Data Integration	The registry must have an ability to integrate with the following systems: 1. Medical Marijuana Seed-to-sale tracking system; 2. Patient Verification system; and 3. Medical Marijuana Business Licensing System		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1u	Change Management	The registry must have the a capability where registered qualifying patient or cardholder can update following information and automatically flag them for internal review prior to approving the change: • A registered qualifying patient to submit changes of address, name, or if the patient ceases to have a debilitating medical condition, within 10 days of change; • A registered designated caregiver to submit changes of the caregiver's name of address, or if the caregiver becomes aware the qualifying patient passed away within 10 days of change; • A registered qualifying patient must notify DOH prior to changing a designated caregiver • A registered qualifying patient to submit changes if a he/she changes a preference as to who may cultivate cannabis for the patient; • The cardholder must notify DOH if he/she loses a card within 10 days of becoming aware the card has been lost; and • A registered qualifying patient must submit changes of a designated dispensary A registry must provide an ability for a designated caregiver to make the required changes on behalf of the registered qualifying patient. Additionally, the registry must flag qualifying patients or caregiver account for internal investigation purposes for the following circumstances caused by changes approved: • A registered qualifying patient who is under 18 years of age to be active in the system without registered caregiver; • A registered caregiver to be active in the system without registered qualifying patient; and • Any other circumstances determined by DOH.		
3.1v	Change Audit	Any changes to information in the registry should be tracked. The audit information should include username, date and time of change, and details of change.		

PATIENT/CAREGIVER REGISTRY				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.1w	ID Card Cancellation/Revocation	DOH personnel must be able to cancel medical marijuana identification card through this portal.		
3.1x	ID Card Renewal	Medical Marijuana identification card will expire in one year or less. This registry must allow Medical Marijuana identification cardholder to renew card by reviewing information, submitting required documents, and pay a renewal fee through the portal. Required documents and renewal fee will be determined by future administrative rules.		
3.1y	ID Reissuance	DOH personnel must be able to reissue identification cards with a new random 10-digit alphanumeric identification number as necessary through this portal. The cardholder must pay $20 fee for reissuance of identification card.		

VERIFICATION				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.2a	Web Based Verification Portal	The verification portal must be a secure web-based system. The verification system must allow law enforcement personnel or medical cannabis establishments to enter a registry identification number or to scan the identification card QR code or barcode to verify the validity of the patient card, caregiver card, medical establishment license, or any medical establishment agent card.		
3.2b	Patient Verification Information	The verification system must disclose only the following information; 1. Whether the identification card is valid; 2. The name of the cardholder; 3. Whether the cardholder is a qualifying patient or a designated caregiver; 4. Whether the cardholder is permitted to cultivate cannabis plants; 5. The registry identification number of any affiliated registered qualifying patient; and 6. The registry identification of the qualifying patient's dispensary or dispensaries, if any.		
3.2c	Establishment and Agent Verification Information	The verification system must disclose only the information regarding medical marijuana agent and establishment that is permitted by future administrative rule.		
3.2d	Portal Configuration	The verification system must be configurable by the system administrator. The system administrators should be able to add or remove searchable fields and information displayed on the verification system.		
3.2e	Data Integration	The verification system must have an ability to integrate with the following systems: 1. Medical Marijuana Seed-to-sale tracking system; 2. Patient Registry system; and 3. Medical Marijuana Licensing System;		

BUSINESS LICENSING				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.3a	Organizational Account	Individuals to create organizational account on behalf of the company to apply for and to renew the medical marijuana establishment licenses.		
3.3b	Individual Account	Individuals to create individual account that is linked to organizational account to apply for medical marijuana agent card.		
3.3c	License Application	The system must allow individual to submit application on behalf of businesses for medical marijuana establishment licenses. The information required for application will be determined by the future administrative rules. The system should provide the copy of the completed application to the applicant.		
3.3d	Agent Application	The system must allow individual to submit application to be a medical marijuana agent. The information required for application will be determined by the future administrative rules. The system should provide the copy of the completed application to the applicant.		
3.3e	Attach Required Documents for Licensing and Agent Cards	The system must allow individuals to submit required documents for medical marijuana establishment licenses or agent card. The documents required for application will be determined by the DOH administrative rules.		
3.3f	Data Validation	The portal must have data validation function to prevent missing data or data type errors. The applications with missing documents should not have submission option in the system.		
3.3g	Fee Collection	Individuals must pay a fee through this portal. The system must allow payment via cash or check.		
3.3h	Fee Adjustment	Allow Fee structure to be adjusted or updated based on legislation or inflation.		
3.3i	Medical Marijuana Agent Card Issuance	The system must issue a medical marijuana agent card. The information listed on the agent card will be determined by the future administrative rules. The vendor must specify the preferred printing software, machine model, and the associated cost in the proposal.		
3.3j	Medical Marijuana License Issuance	The system must issue a medical marijuana establishment license. The information listed on the license will be determined by the future administrative rules.		

BUSINESS LICENSING				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.3k	Medical Marijuana Establishment Dashboard	Provide a dashboard where individuals can see the status of their application for licenses or agent card associated with their business.		
3.3l	Communication	Provide a communication feature to send automatic notification and alerts to licensees and agent cardholders. The portal must provide a communication feature where DOH staff can directly communicate with specific applicants in a secure manner. The record of communication between the DOH personnel and applicant or licensee should be stored and reviewable in the system. The communication record should include sender, recipient, date and time of communication, and the content of the communication.		
3.3m	Department Review of Applications	Allow DOH personnel to review, accept, or deny the applications.		
3.3n	Internal Edits	DOH staff should have ability to edit application records. The edit capability should be provided to certain personnel based on their security role in the registry system to maintain adequate internal control and data integrity.		
3.3o	Internal Dashboard	Provide a dashboard where DOH staff can see the list of application to be reviewed. The dashboard should provide sort and filter feature where internal staff can organize the applications.		
3.3p	Internal Workflow	This portal should have ability to automatically move applications through the process set by DOH from application submission to the card or license issuance. The portal should assign application to appropriate DOH personnel based on role set in the system with ability to manually select applications for review or approval. DOH personnel should receive alerts or notification when applications are assigned to them. Additionally, the workflow should include violation queue where DOH personnel can manually assign incomplete applications to streamline the workflow process to ultimately yield completed applications.		

BUSINESS LICENSING				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.3q	Data Import and Export	Export data in the system in CSV or Excel format. The portal must provide the ability to create custom reports based on selected fields, and the ability to save certain reports to reduce redundancies.		
3.3r	Information Sharing with Local Government Entities	The system must be able to have method to share certain application information with applicable local government personnel. This includes an ability to create specific security role for local government personnel.		
3.3s	Licensing Reporting	The system must have reporting functionality with easy-to-use query function. The portal must have reporting tool with sort and filter function, an ability to save and share custom report specification, and an ability to export the report in various formatting including Microsoft Excel or PDF. The system should also come with templates of reports including but not limit to the following list: • Total number of application received for medical marijuana agent cards and medical marijuana establishment licenses by license type • Total number of approved application for medical marijuana agent cards and medical marijuana establishments by establishment type • The number of revocations • List of newly approved medical marijuana establishment licenses by license type • The percentage breakdown of medical marijuana establishments • Total fees collected for licenses and agent cards • The total number of designated patients and their physicians information by dispensary The template reports should contain the latest data at the time of export, with the ability to set the date range for the reports.		

BUSINESS LICENSING				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.3t	Data Integration	The registry must have an ability to integrate with the following systems: 1. Medical Marijuana Seed-to-sale tracking system; 2. Verification system; and 3. Medical Marijuana Patient and Caregiver Registry		
3.3u	Change Management	The system must have a capability where qualified individuals or licensee can submit changes and automatically flag them for internal review prior to approving the change. The list of information that can be changed by the agent cardholder or licensee will be determined by the future administrative rules.		
3.3v	Change Audit	Any changes to information in the portal should be tracked. The audit information should include username, date and time of change, and details of change.		
3.3w	Agent Card Cancellation/Revocation	DOH personnel must be able to cancel medical marijuana agent card through this system if necessary.		
3.3x	Agent Card Renewal	The Medical Marijuana agent card must have an expiration date. This system must allow Medical Marijuana agent to renew card by reviewing information, submitting required documents, and pay a renewal fee through the portal. Required documents, renewal period and fee will be determined by the future administrative rules.		

BUSINESS LICENSING				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REFERENCE
3.3y	Agent Card Reissuance	DOH personnel must be able to reissue agent cards as necessary through this system. The fee for reissuance will be determined by the future administrative rules.		
3.3z	License Cancellation/Revocation	DOH personnel must be able to cancel medical marijuana establishment licenses through this system if necessary.		
3.3aa	License Renewal	The Medical Marijuana Establishment Licenses must have an expiration date. This system must allow Medical Marijuana Establishment licensee to renew card by reviewing information, submitting required documents, and pay a renewal fee through the portal. Required documents, renewal period and fee will be determined by the future administrative rules.		
3.3ab	License Reissuance	DOH personnel must be able to reissue licenses as necessary through this system. The fee for reissuance will be determined by the future administrative rules.		
3.3ac	Inspection Scheduling	OPTIONAL: The system to provide a randomized scheduling feature. This feature allows a random date selection of inspection date that can be manually adjusted by the inspectors if necessary.		
3.3ad	Packaging Approval Application	**OPTIONAL:** The system allows individual to submit application on behalf of businesses for marijuana product packaging approval. The information required for application will be determined by the future administrative rules. The system should provide the copy of the completed application to the applicant.		
3.3ae	Packaging Document Upload	**OPTIONAL:** The system allows individuals to submit required documents for product packaging approval including but not limited to the picture of the packaging and labels. The documents required for application will be determined by the DOH administrative rules.		

SECURITY & MAINTENANCE						
			ENTER YES/NO			
ID	CATEGORY	REQUIREMENT	PATIENT REGISTRY	VERIFICATION	BUSINESS LICENSING	PAGE REFERENCE
3.4a	State Single Sign on	As part of the State's Identity and Access Management (IAM) strategy, the proposed system must integrate with the State of South Dakota's standard identity management service (SSO) which enables custom control of how citizens and/or state employees sign up, sign in, and manage their profiles. The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0. This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users. If the vendor is not able to fulfil this identity management standard, they will be considered disqualified and the proposal will not be evaluated.				
3.4b	Hosting and Data Access	The vendor must agree that the State will own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms. DOH will give preference to vendors who can provide a cloud-based solution hosted/deployed onto the States' Microsoft Azure Cloud Tenant or a States preferred platform.				
3.4c	Data Hosting Option	The vendor may provide state-hosted option and/or vendor hosted option in the proposal. The vendor hosted option must include the current server/system, specifications, software, and versions.				
3.4d	Web-based services	The application(s) must have secure web-based access. The application(s)must be accessible through various internet browser including Mozilla Firefox, Google Chrome, and				

		Microsoft Edge. The application(s) must also be mobile friendly.				
SECURITY & MAINTENANCE						
			ENTER YES/NO			
ID	CATEGORY	REQUIREMENT	PATIENT REGISTRY	VERIFICATION	BUSINESS LICENSING	PAGE REFERENCE
3.4e	System Upgrades	The proposal must include system upgrade plan that includes but not limited to: upgrade plan, types and frequency of upgrades. The purpose of this plan is to ensure that the proposed solution(s) have upgrade procedures that creates minimal impact or interference on system availability.				
3.4f	System Issue Communication	The application(s) must have an alert system where both external and internal users receive notification in case of system outage with estimated time needed for repair.				
3.4g	System Maintenance	The application(s) must have a periodic maintenance to update the system, fix any known issues, and address requested improvements.				
3.4h	Data Security	The data security for the proposed solution (s) must meet the requirements set by the State and HIPPA.				
3.4i	User Role Permissions	User Roles must limit CRUD (Create, Read, Update, Delete) access per Role. Addition of new Roles and changes to Role CRUD access must be easy.				
3.4j	Data Encryption	The application(s) must utilize data encryption when data is sent				
3.4k	Sensitive Data Storing	The application(s) must not store authentication credentials or sensitive data in its code.				

SECURITY & MAINTENANCE						
			ENTER YES/NO			
ID	CATEGORY	REQUIREMENT	PATIENT REGISTRY	VERIFICATION	BUSINESS LICENSING	PAGE REFERENCE
3.4l	Interfaces and Integration	The vendor must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, DOH expects that the vendor will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the Proposal.				
3.4m	Data normalization	The application(s) will have the ability of data normalization to reduce and eliminate data redundancy.				
3.4n	Design Pattern	The application permissions will follow an "explicitly granted" design pattern.				
3.4o	Environment	The application(s) will require close/separate environments for: development, testing and production				
3.4p	Session Timeouts	The application(s) will enforce session timeouts during periods of inactivity.				
3.4q	Credential Storing	The application(s) will not store authentication credentials or sensitive data in its code.				
3.4r	Change Management Documentation	The application(s) will utilize change management documentation and procedures.				
3.4s	Customer Support	The vendor must provide technical and end-user support via phone and email from Monday through Friday, 7:00 AM to 6:00 PM CST. Additionally, the vendor must be available and has ability to respond to critical issues in timely fashion regardless of the time of the incident.				

SECURITY & MAINTENANCE						
			ENTER YES/NO			
ID	CATEGORY	REQUIREMENT	PATIENT REGISTRY	VERIFICATION	BUSINESS LICENSING	PAGE REFERENCE
3.4t	Support and Maintenance Plan	The proposal must include system update plan. The plan at minimum must include the following items: 1. Testing: Provide the testing plan that describes a plan for user acceptance training, development of user acceptance testing environment, stress regression, and performance test plan. 2. Implementation: Provide the implementation plan of the application that describes how the implementation is prioritized, planned, managed, and executed. 3. Ongoing Maintenance: Provide maintenance plan that describe level of support service provided with estimated response time. 4. Modification: Provide methodologies for how modifications are charged to the State. 5. Seed-to-sale integration: Provide Seed-to-sale integration plan which includes information on whether the vendor has their own seed -to-sale tracking or if they have an external seed-to-sale tracking that integrates with proposed solutions.				
3.4u	Mobile Application	**OPTIONAL:** The proposed solution offers a mobile application experience that works on the most popular mobile platforms and is targeted for use by Law Enforcement Officers and Medical Marijuana Establishment Employees.	NA		NA	
3.4v	Barcode Reader	**OPTIONAL:** The proposed solution offers a mobile app experience that features a barcode scan feature compatible with state documents (e.g. driver's license) for use by Law Enforcement Officers and Medical Marijuana Establishment Employees.	NA		NA	

OPERATION						
			ENTER YES/NO			
ID	CATEGORY	REQUIREMENT	PATIENT REGISTRY	VERIFICATION	BUSINESS LICENSING	PAGE REFERENCE
3.5a	3 Components Bid	The vendor must submit a bid for all three components of this RFP: Patient Registry, Verification, and Business Licensing. A proposal that does not contain all three components will be considered disqualified and the proposal will not be evaluated.				
3.5b	Previous Government Experience	The vendor must provide a minimum of 2 example of a successful software implementation of a system similar to this RFP and 3 references from governmental agencies.				
3.5c	Legislative Updates	The vendor must provide legislative and regulatory updates within the scope of the proposed 5-year bid/contract at no expense to the State				
3.5d	Law Enforcement Access	Provide an access or integration plan that allow state and local law enforcement officers to securely access the verification system.	NA		NA	
3.5e	Risk Management and Communication Plan	The vendor must provide a written risk management and communication plan for the proposed 5-year term of the contract.				
3.5f	Training Plan	The vendor must provide a training plan for both internal and external users. Training plan should include the following items and estimated completion timeframe for each of the item: • Training Needs Analysis • Role Based Training Materials • Webinar Based Training • End User Manual and Material Updates • Periodic Training Assessment Review				

4. PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 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.

4.2 The offeror may be required to submit a copy of their most recent audited financial statements upon the State's request.

4.3 **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.

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

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

5. FORMAT OF SUBMISSION

5.1 1 original, 1 electronic copy, and 1 electronic copy with propriety information redacted of the proposal must be submitted.

I. The electronic copy should be provided in MS WORD or in PDF format. The submission must be delivered as indicated in Section 1.6 of this document.
II. The Proposals must clearly identify which hosting option is being proposed. The proposal must include a separate section for each hosting option if the vendor is submitting proposals for both options.
III. The proposal must include a separate section for each component of the RFP.
IV. The proposal should be page numbered and should have an index and/or a table of contents.

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

I. **RFP Form:** The State's Request for Proposal form completed and signed.
II. **Executive Summary:** The one- or two-page executive summary 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.
III. **Response to the Requirement Listing (Section 3.1 – 3.5 of the RFP):** The

response to the list of requirements with reference page number from the proposal completed.

IV. **Detailed Response:** This section should constitute the major portion of the proposal and must contain at least the following information:
    a. 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.
    b. 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.
    c. A clear description of any options or alternatives proposed.

V. **Cost Proposal:** All interested vendors must submit the Appendix B Cost Sheet. All costs related to the provision of the required services must be included in each cost proposal offered. Vendors may submit cost proposals in addition to the required cost sheet. The separate cost proposals should be submitted for each of the component and for each of the data hosting option. Furthermore, the offeror shall submit a statement in the Cost Proposal that attests the offeror's willingness and ability to perform the work described in this RFP for the price being offered.

VI. **Security and Vendor Questions**: All interested vendors must submit the Appendix D Security and Vendor Questions. If the contractor answers a question by referencing another document or another part of the RFP response, they must give the page number and paragraph where the information can be found.

The offeror may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State for allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies, or excessive resource consumption. The cost for additional work chargeable to the State should be included in your proposal.

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.

Offerors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

5.3 Statement of Understanding of Project

Please summarize your understanding of what work is being requested in this proposal and what the work will entail. This should include, but not be limited to, your understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and your understanding of the deliverables. Your specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements should be included. This section

should be limited to no more than two pages.

6. PROPOSAL EVALUATION AND AWARD PROCESS

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

Required Proposal Evaluation Criteria	
Category	**Percentage**
Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements.	30%
Resources available to perform the work, including any specialized services, within the specified time limits for the project.	25%
Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration	15%
Availability to the project locale	5%
Familiarity with the project locale	5%
Proposed project management techniques	10%
Ability and proven history in handling special project constraints	10%
Total	100%

Additional Proposal Evaluation Criteria	
Category	**Percentage**
Essential: If the proposal does not meet these requirements, the proposal will be automatically disqualified. **For this RFP, the only essential requirements are single sign on, and 3 components bid.**	
Communication: evaluates the proposed system's ability to accommodate secure and direct communication between the department staff and customers, and system-wide alerts for any potential issues or important information. A system with easy-to-use system wide communication features and the ability to directly communicate with the appropriate end users will score higher for this criterion.	5%
Integration: evaluates the proposed system's ability to smoothly integrate with various systems required for Medical Marijuana program.	10%
Operation: evaluates proposed system's ability to provide functionality and flexibility required for South Dakota Medical Marijuana program. A system with flexible features that ensures data accuracy and streamlines internal workflow will score higher for this criterion.	15%
Reporting: evaluates proposed system's ability to provide both template and custom reporting to meet the various reporting needs. The custom reporting function that is flexible and easy to use will score higher for this criterion.	10%
System Design: evaluates the foundational system design of the proposed system. These are including, but not limited to, account creation, document upload, and card or license issuance.	20%

Security: evaluates proposed system's various security features and level of security offered as a safeguard to protect sensitive data.	15%
Support and Maintenance evaluates the level and types of customer support and maintenance plan offered for the proposed system. The support and maintenance plan that provides clear timeline and deliverables, as well as clear expectation of turnaround time for maintenance and support will score higher for this criterion.	10%
Training: evaluates the training plan. The training plan that includes a detailed timeline of training with clear expectations of deliverables will score higher for this criterion.	5%
Cost: evaluates the proposed cost	10%
Total	100%

Vendor Presentation Evaluation Criteria	
Category	**Percentage**
Ease of Use: evaluates the use friendliness of the proposed system. The system that is intuitive and easy to navigate will score higher for this criterion	30%
Product Functionality: evaluates various functionality that fulfills the requirement listed in the RFP. This also evaluates additional or optional functionality that is unique to the proposed system	30%
Flexibility: evaluates the flexibility of functionality and process within the proposed system. The system that can accommodate to unique needs to South Dakota Medical Marijuana program will score higher for this criterion.	30%
Adherence to Use Cases: evaluates the preparedness of each vendor. The vendor that is well prepared and thoroughly demonstrate the Use Cases will score higher for this criterion	10%
Total	100%

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

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

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

6.5 Award

The requesting agencies 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.

1. If the agencies 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 agencies, the agencies shall, either orally or in writing, terminate negotiations with the offeror. The agencies may then negotiate with the next highest ranked offeror.
2. The negotiation process may continue through successive offerors, according to the evaluation score by rank, until an agreement is reached, or the agencies terminate the contracting process.

7. BEST AND FINAL OFFERS

The State reserves the right to request best and final offers. If so, the State will initiate the request for best and final offers; best and final offers may not be initiated by an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which offerors will be notified and provide them an opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If an offeror does not submit a best and final offer or a notice of withdrawal, the offeror's previous proposal will be considered that offeror's best and final proposal. After best and final offers are received, final evaluations will be conducted.

8. SCANNING

8.1 The Offeror acknowledges that the State will conduct a security and vulnerability scan as part of the review of the Offeror's RFP if the offeror is hosting. This scan will not include a penetration test. The State will use commercially available, industry standard tools to scan a non-production environment with non-production data at mutually agreeable times.

8.2 The Offeror should fill out the form in Appendix E and sign the form. The Offeror's employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given, the State will assume that the State can scan at any time. At the State's option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved, the State is more likely to consider a security scan necessary for an RFP to be considered. Except for State staff, the State will only provide scan information to the Offeror's security contact. At the State's option, the State will conduct the scan at a location named by the Offeror. The Offeror can only request, not require naming the scanning location. The State may consider a comprehensive, complete, and recent risk assessment as satisfying the scanning requirement. If required, the State will sign a non-disclosure agreement before scanning or receiving the risk assessment.

9. ADDITONAL CLAUSES AND AGREEMENT TERMS

9.1 Any contract or agreement resulting from this RFP will include Security Acknowledgement Form and Business Associate Agreement along with the State's standard I/T contract terms. As part of the negotiation process, the contract terms listed within the RFP and Appendix C may be altered or deleted.

The Offeror should declare in their response any issues they have with specific contract or agreement terms. If the Offeror does not declare that there are any issues with any contract terms, then the State will assume those are acceptable to the Offeror.

APPENDIX A – Use Cases for Vendor Presentation

The use cases outlined below must be demonstrated by vendors that are invited to participate in oral presentation. The purpose of the use cases is to evaluate the usability of the software and to determine which software would be the best fit for the South Dakota Medical Marijuana Program. Each vendor is solely responsible for demonstrating appropriate use cases based on their proposal.
Additionally, each vendor may present any additional features that are unique to the proposed system.
Each vendor will have one hour for presentation, and one hour of Q&A section. The maximum time allotted for each vendor is two hours. The Oral Presentation/User Case Demonstration will be evaluated based on the following criteria:

1. Ease of Use: evaluates the use friendliness of the proposed system. A system that is intuitive and easy to navigate will score higher for this criterion.
2. Product Functionality: evaluates various functionality that fulfills the requirement listed in the RFP. This also evaluates additional or optional functionality that is unique to the proposed system.
3. Flexibility: evaluates the flexibility of functionality and process within the proposed system. The system that can accommodate to unique needs to South Dakota Medical Marijuana program will score higher for this criterion.
4. Adherence to Use Cases: evaluates the preparedness of each vendor. The vendor that is well prepared and can thoroughly demonstrate the Use Cases will score higher for this criterion.

Administrative Use Cases: The vendors must demonstrate the following administrative use cases for patient registry and business licensing software.

1. Role Based Security

User	System Administrator
Basic Process	1. Navigate to user permissions 2. Add a new security role 3. Add a permission to a security role 4. Assign a security role to the user 5. Delete a permission to a security role

2. Fee Adjustment

User	Department Staff
Basic Process	1. Navigate to the fee listing page 2. Adjust the fee amount 3. Supervisor approves the fee change

3. Department Workflow - Reviewer

User	Department Staff
Basic Process	1. Navigate to the internal workflow dashboard 2. Move application to the queue 3. Review the application 4. Review Uploaded document 5. Approve or Deny the application

4. Department Workflow – Auto Assign

User	Department Supervisor
Basic Process	1. Navigate to the internal workflow dashboard 2. Review the applications that are auto assigned to the specific reviewer 3. Change the reviewer assignment for one application manually

5. Department Workflow – Supervisor

User	Department Supervisor
Basic Process	1. Navigate to the internal workflow dashboard 2. Navigate to Supervisor queue 3. Review application that has missing doctor's recommendation 4. Deny the application and send it back to the reviewer and communicate the reason for the denial to the reviewer

6. Reporting

User	Department Staff and Supervisors
Basic Process	1. Navigate to reporting page 2. Run template report 3. Create a custom report by selecting fields 4. Export it to Microsoft Excel or csv

7. Card Issuance and Example of Cards

User	Department Staff and Supervisors
Basic Process	1. Navigate to card issuance page 2. Verify information and picture 3. Issue a card

8. Audit Trail

User	Department Supervisor
Basic Process	1. Navigate to audit trail page 2. Select one audit record and review the detail 3. Export the audit trail data for certain week to Microsoft Excel or csv

Patient Registry

1. Patient Application

User	Patient
Basic Process	1. Navigate to registry website 2. Create an account 3. Enter information on the application 4. Enter Caregiver information 5. Attach required documents 6. Pay a fee 7. Submit an application

2. Caregiver Application

User	Caregiver
Basic Process	1. Navigate to registry website 2. Create an account 3. Enter information on the application 4. Enter Patient information 5. Attach required documents 6. Pay a fee 7. Submit an application

3. Review Multiple Caregiver Application for the Same Patient

User	Department Staff
Basic Process	1. Navigate to application listing 2. Review Caregiver applications 3. Check the patient association 4. Enter number of permitted home grow 5. Approve one caregiver 6. Deny another caregiver application for the same patient and send a communication to the applicant

Verification

1. Verification of Patients, Caregiver, and Agents

User	Dispensary Employee and/or Law Enforcement Officers
Basic Process	1. Navigate to verification page 2. Enter Patient identification number 3. Review the information and check the validity of the card

2. Configure the Search Function:

User	Department Staff
Basic Process	1. Navigate to configuration page 2. Remove the ability to search using mailing address 3. Limit searchable fields to identification number

Business Licensing

1. Medical Marijuana Establishment License Application

User	Medical Marijuana Establishment Owners or Employees
Basic Process	1. Navigate to licensing website 2. Create an account 3. Enter information on the application 4. Attach required documents 5. Pay a fee 6. Submit an application

2. Medical Marijuana Agent Application

User	Medical Marijuana Establishment Owners or Employees
Basic Process	1. Navigate to licensing website 2. Create an account 3. Enter information on the application 4. Select Establishment to be associated 5. Attach required documents 6. Pay a fee 7. Submit an application

4. Review Multiple Agent Application for the Same Establishment

User	Department Staff
Basic Process	1. Navigate to application listing 2. Review agent applications 3. Check the establishment association 4. Approve one agent 5. Change the business association of another agent and deny the application 6. Send communication to the applicant whose application has been denied

5. Share Establishment Application with Local Government Personnel

User	Local Government Staff
Basic Process	1. Log into a licensing software 2. Review the licensing applications that are specific to the jurisdiction 3. Export the application and required documents to pdf or Microsoft word

APPENDIX B – Cost Sheet

All interested vendors must fill out this cost sheet to provide a clear cost estimate for this RFP. Vendors may include additional cost proposal details in the proposal to supplement the information on the cost sheet.
Cost should be clearly marked, and the cost structure should be clearly explained on this sheet.
Because a proposal may be submitted for one hosting option or both options, all interested vendors must fill applicable fields on this cost sheet based on the proposal.
Vendors may request a separate electronic copy of this form for use in completing their cost proposal.

1. **Basic Cost:** the cost for this section should cover the implementation and ongoing maintenance and support for all the requirements outlined in Section 3.1 through 3.5 of this RFP.

Vendor Hosted: Patient Registry	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

State Hosted: Patient Registry	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

Vendor Hosted: Verification System	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

State Hosted: Verification System	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

Vendor Hosted: Business Licensing	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

State Hosted: Business Licensing	Dollar Amount
Implementation Cost	
Ongoing Support and Maintenance Cost	
Year 1	
Year 2	
Year 3	
Year 4	
Year 5	
Total	

2. **Cost Structure Explanation:** Please provide an explanation of the cost structure for this component. If the structure is the unit pricing model or tier pricing model, the cost per unit or tier should be provided.

a) Patient Registry

Explanation	
Cost per Unit or Per Tier	

b) Verification System

Explanation	
Cost per Unit or Per Tier	

c) Business Licensing

Explanation	
Cost per Unit or Per Tier	

3. **Optional Cost:** the cost for this section should cover the implementation and ongoing maintenance and support for requirements that are labeled as optional. Any additional features that are unique to your proposal and the cost associated with them should be included in this section.

Vendor Hosted: Optional Services	Dollar Amount
a.	
b.	
c.	
d.	
e.	
f.	
g.	
h.	

State Hosted: Optional Services	Dollar Amount
a.	
b.	
c.	
d.	
e.	
f.	
g.	
h.	

APPENDIX C - Bureau of Information and Telecommunications Required Contract Terms

1.0 BIT STANDARD STATE CONTRACT TERMS

1.1 CONFIDENTIALITY OF INFORMATION:

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

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

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

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

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

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

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Vendor understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. 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.

1.2 CYBER LIABILITY INSURANCE:

The Vendor shall maintain cyber liability insurance with liability limits in the amount of $10 million dollars 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 shall 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 shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor shall furnish copies of insurance policies if requested by the State. The insurance will stay in effect for 2 years after the work covered by this agreement is completed.

1.3 CHANGE MANAGEMENT PROCESS:

From time to time it may be necessary or desirable for either the State or the Vendor to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Vendor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Vendor on a schedule no less favorable than that provided by the Vendor to any other customer receiving comparable levels of services.

1.4 WORK PRODUCTS:

The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and

coordination of all services furnished by the Vendor and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Vendor to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Vendor shall, without additional compensation, correct or revise any errors or omissions in its work products.

Vendor hereby acknowledges and agrees that all State Proprietary Information, any information discovered by the State, Personally Identifiable Information (PII), data protected under Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information defined under state statute as confidential, and all information contained therein provided to the State by the Vendor in connection with its performance under this Agreement shall belong to and is the property of the State and will not be used in any way by the Vendor without the written consent of the State.

1.5 PRODUCT CONFORMITY:

The State has twelve (12) months following final acceptance of the product(s) delivered by the Vendor pursuant to this Agreement to verify that the product(s) conform to the requirements of this Agreement and perform according to the Vendor's system design specifications. Upon the State's recognition of an error, deficiency, or defect, the Vendor shall be notified by the State. The notification shall cite any specific deficiency (deficiency being defined as the Vendor having performed incorrectly with the information previously provided by the State, not the Vendor having to modify a previous action due to additional and/or corrected information from the State). The Vendor, at no additional charge to the State, shall provide a correction or provide a mutually acceptable plan for correction within thirty-days following the receipt of the State's notice to the Vendor. If the Vendor's correction is inadequate to correct the deficiency, or defect, or if error recurs, the State may, at its option, act to correct the problem. The Vendor shall be required to reimburse the State for any such costs incurred or the State will consider this to be a breach of the agreement. Payment by the Vendor pursuant to this provision does not waive any other rights and remedies available to the State.

1.6 UNRESOLVED BREACH OF THE AGREEMENT

In the event of an unresolved breach of this agreement, the parties acknowledge that damages from the breach will be difficult or impossible to measure or quantify. The parties agree that in the event of a breach, the Consultant shall pay, as liquidated damages, and not as a penalty, the sum of $ _____ or the amount paid by the State to the Consultant plus ___ %, whichever is less which the parties agree is a fair and reasonable method of computing the damages caused by the breach.

1.7 CURING OF BREACH OF AGREEMENT:

In the event of a breach of these representations and warranties the State may, at the State's discretion, provide the Vendor with the opportunity to rectify the breach. The Vendor shall immediately, after notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Vendor's request, a written notice to reaffirm the telephonic notice. If such problem remains unresolved after three days, at State's discretion, Vendor will send, at Vendor's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the

site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

1.8 DOMAIN NAME OWNERSHIP:

Any website(s) that the Vendor creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Vendor is providing a service that utilizes a website with the domain name owned by the Vendor, the Vendor must give thirty (30) days' notice before abandoning the site. If the Vendor intends to sell the site to another party the Vendor must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Vendor or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

1.9 SOFTWARE FUNCTIONALITY AND REPLACEMENT:

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

The solution will be used to register and verify medical marijuana patients and designated caregivers. It will also be used to register medical marijuana businesses and to manage the necessary interactions between the state and applicants/registrant businesses.

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 shall 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 shall 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.

1.10 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 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.

1.11 LICENSE GRANT:

A. The Vendor grants to the State a worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this agreement.

B. The license usage model is based on a future known number of internal state users that will fluctuate over time, an unknown number of external public users that cannot reasonably be predicted, and an unknown number of external law enforcement users that will fluctuate and cannot be predicted at any given time.

C. The license grant may be extended to any contractors, subcontractors, outsourcing Vendors and others who have a need to use the software for the benefit of the State.

1.12 SOURCE CODE ESCROW:

A. Deposit in Escrow: "Source Code" means all source code of the Software, together with all commentary and other materials supporting, incorporated into or necessary for the use of such source code, including all supporting configuration, documentation, and other resource files and identification by Vendor and version number of any software (but not a license to such third-party software) used in connection with the source code and of any compiler, assembler, or utility used in generating object code.

1. Within ninety (90) days of the effective date, Vendor shall deposit the Source Code for the software with a nationally recognized software escrow company (subject to the approval of the State, not to be unreasonably withheld) (the "Escrow Agreement"). Within thirty (30) days after delivery to Customer of any major update, Vendor shall deposit the Source Code for such update with the Escrow Agent pursuant to the Escrow Agreement. For all other updates, Vendor shall deposit the Source Code for such updates on a semiannual basis with the Escrow Agent pursuant to the Escrow Agreement.

2. The parties agree that the Escrow Agreement is an "agreement supplementary to" the Agreement as provided in Section 365(d) of Title 11, United States Code (the "Bankruptcy Code"). Immediately upon termination of this Agreement, the Source Code shall be released back to Vendor.

B. Conditions for release: The State will have the right to obtain the Source Code in accordance with and subject to the terms and conditions of this Section and the Escrow Agreement provided that all of the following three conditions are met (collectively a "Release Event"):

1. Vendor winds down its business or liquidates its business under a Chapter 7 Bankruptcy proceeding; or Vendor discontinues maintenance and support to the Software,

2. No entity has succeeded to Vendor's obligations to provide maintenance and support on the Software in accordance with the Agreement in effect between the parties, and

3. The State is not in breach of its obligations under this Agreement.

C. Source Code: In no event shall the State have the right to use the Source Code "barring a release event" for any purpose, and the State is specifically prohibited from using the Source Code to reverse engineer, develop derivative works or to sublicense the right to use the Source Code to any other person or entity for any purpose. Customer will also be obligated to treat the Source Code as Confidential Information of Vendor under the Agreement.

The cost for establishing and maintaining the Escrow Account will be that of the State.

1.13 FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:

The Parties agree that the State shall 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.

1.14 DATA RECOVERY:

The Consultant must be able to recover the State's data in the same state it was sent to the Consultant for 13 months. If the Consultant system or the third-party system that is hosting data for the Consultant is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the State data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the State and the Consultant.

1.15 REJECTION OR EJECTION OF VENDOR, AND VENDOR'S SUBCONTRACTORS, AGENTS, ASSIGNS AND/OR AFFILIATED ENTITIES EMPLOYEE(S):

The State, at its option, may require the vetting of the Vendor, and any of the Vendor's Subcontractors, Agents, Assigns and/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 shall immediately remove the individual from the project.

1.16 THREAT NOTIFICATION:

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 (2) business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Vendor.

1.17 SECURITY INCIDENT NOTIFICATION:

For protected non-health information only, 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 Policies found at: https://bit.sd.gov/vendor/default.aspx. The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the 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 shall notify the State Contact within twelve (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 twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

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

C. At the State's discretion, the Vendor must provide to the State all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the Security Incident: (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered: (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none, use AES256 encryption. Vendor shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

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

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

1.18 HANDLING OF SECURITY INCIDENT:

For Security Incidents of protected non-health information under the Vendor's control and 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:

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

If, at the State's discretion the Security Incident was due to the actions or inactions of the 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 shall offer 3 years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Vendor, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the 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 twelve (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 shall 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.

1.19 SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION:

Security Incident means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. The Vendor shall alert the State Contact within twelve (12) hours of a Security Incident and provide daily updates to the BIT contact at their

request. The Parties agree that this alert does not affect the 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 Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the 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 shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the Vendor is responsible for the Security Incident, the Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Vendor's services and/or product(s).

1.20 ADVERSE EVENT:

The Vendor shall notify the State Contact within two (2) 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.

The Vendor also acknowledges that if not kept secure, the State's data could be, in aggregate, used for illegal purposes.

Except as mandated by other legal requirements the Vendor shall provide notice of the disclosure only to the State. Notification to the State of an Adverse Event involving the disclosure of State Data shall consist of:

i. a description of the data disclosed;
ii. the time the disclosure occurred, and;
iii. a general description of the circumstances of the disclosure.

If all this information is not available for the notification within the specified time, the Vendor shall provide the State with all the available information along with the reason for the incomplete notification.

The parties agree with respect to any Adverse Event that the Vendor shall at its sole expense:

i. promptly and fully investigate the cause of the Adverse Event;
ii. cooperate fully with the State's investigation of, analysis of, and response to the incident;
iii. Take all reasonable steps to mitigate any harm caused to affected individuals and/or entities and to prevent any future reoccurrence;
iv. provide the State with documentation of responsive actions taken related to the disclosure, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement, and;
v. comply with applicable data breach notification laws, including without limitation the provision of credit monitoring and other fraud prevention measures, for a period of twelve (12) months from the date that Vendor notifies Customer of the Adverse Event.

The State will determine if notification to individuals or entities other than the State is required and if the notification will be carried out by the State or by the Vendor. The method and content of the notification of the affected parties will be subject to approval by the State.

At the State's discretion and at the Vendor's expense the Vendor may be required to use a credit monitoring service, call center, and/or a forensics company.

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 the notification, investigation and remediation of the disclosure.

1.21 BROWSER:

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

1.22 SECURITY ACKNOWLEDGEMENT FORM:

The Vendor will be required to sign the Security Acknowledgement form which is attached to this Agreement as Appendix F. The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This form constitutes the agreement of Vendor to be responsible and liable for ensuring that the Vendor, Vendor's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy- Contractor Version (ITSP) found at https://bit.sd.gov/vendor/default.aspx . 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, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Vendor's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Vendor and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

1.23 BACKGROUND CHECKS:

The State requires all employee(s) of the Vendor, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of both the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Vendor, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks

must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Vendor with notice of this determination.

1.24 INFORMATION TECHNOLOGY STANDARDS:

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

1.25 SECURITY:

The Vendor shall 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 and Medium can be described as follows:

a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.

b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.

c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.

d. **Low-** Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.

B. Assistance will be provided to the State by the 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.

C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

D. All members of the development team have been successfully trained in secure programming techniques.

E. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

F. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at http://bit.sd.gov/standards/.

G. The Vendor will fully support and maintain the Vendor's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Vendor may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Vendor's application to a new release of third-party technology if:

i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and

ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Vendor may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.

If a code base or platform on which the Vendor's application depends is no longer supported, maintained, or patched by a qualified third party the Vendor commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Vendor to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

1.26 MALICIOUS CODE:

a. The Vendor warrants that the service/ licensed software contains no code that does not support an application requirement.

b. The Vendor warrants that the service/ licensed software contains no malicious code.

c. The Vendor warrants that the Vendor will not insert into the service/ licensed software or any media on which the service/ licensed software is delivered any malicious or intentionally destructive code.

d. The Vendor warrants that the Vendor will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the service/ licensed software before installation. In the event any malicious code is discovered in the service/ licensed software delivered by the Vendor, the Vendor shall provide the State at no charge with a copy of the applicable service/ licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

1.27 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 shall enter into a contract with one or more service providers for payment card services under this Agreement. The Vendor shall 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 shall 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.

1.28 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.

1.29 PAYMENT CARD INDUSTRY QUALIFICATION REQUIREMENTS FOR QUALIFIED INTEGRATORS AND RESELLERS:

When having a payment card application implemented, configured and or supported the Vendor and any subcontractor(s) used by the Vendor to fulfil the terms of this contract 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.

1.30 LICENSE AGREEMENTS:

Vendor warrants that it has provided to the State and incorporated into this Agreement all

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

1.31 WEB AND MOBILE APPLICATION:

The Vendor's application is required to;

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

N. if any health or medical information is gathered or accessed by this application that is not protected by HIPAA and HITECH rules and regulations then the opening screen must state, in an easy to read font that the application is gathering and or accessing health and or medical information and the user's privacy is not protected by federal regulations; and
O. any application to be used on a mobile device must be password protected.

The Vendor is required to disclose all:

A. functionality;
B. device and functional dependencies;
C. third party libraries used;
D. methods user data is being stored, processed or transmitted;
E. methods used to notify the user how their data is being stored, processed and or transmitted;
F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted;
G. methods used to record the user's response(s) to the notification that their data is being stored, processed and or transmitted;
H. methods used to secure the data in storage, processing or transmission; and
I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
J. methods used to create and customize existing reports;
K. methods used to integrate with external data sources;
L. methods used if integrates with public cloud provider;
M. methods and techniques used and the security features that protect data, if a public cloud provider is used; and
N. 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.

1.32 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

1.33 OFFSHORE SERVICES:

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 the written

permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

1.34 MULTIFACTOR AUTHENTICATION:

The Vendor's and the Vendor's subcontractors will not access the State's network except through the State's Multifactor Authentication process. For purposes of remote access to the State systems on the State's domain, the Vendor will adhere to the State's requirements for Multifactor Authentication upon receipt of notification from the State that such requirements have been implemented. The Vendor will also require adherence to the State's requirements by any of the Vendor's officers, employees, subcontractors, agents, assigns, and affiliated entities who will have remote access to State systems on the State's domain. The State's requirements for Multifactor Authentication are set forth in the State's Information Technology Security Policy, which is attached as Appendix.

1.35 VENDOR'S SOFTWARE LICENSES:

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

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

1.37 DATA SANITIZATION:

At the end of the project covered by this Agreement the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most

current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the 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. The only exceptions are when the State Data must be maintained after the project is completed for legal reasons or the State data is on a backup medium where the State data cannot be separated from other data. If the state data cannot be sanitized for these reasons, then the Vendor must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.

This contract clause remains in effect for as long as the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities have the State data, even after the Agreement is terminated or the project is completed.

1.38 BANNED HARDWARE:

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, Huwaei 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.

1.39 USE OF PORTABLE DEVICES:

The Vendor shall prohibit its employees, agents, affiliates, and subcontractors form 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.

1.40 REMOTE ACCESS:

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

×

1.41 STATE OF SOUTH DAKOTA TECHNOLOGY OVERSIGHT:

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. BIT requires the contract provisions which are attached to this Agreement as Appendix C and incorporated into this Agreement by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only Appendix C of this agreement. Before renewal of this Agreement BIT must review and approve Appendix C as still being current. BIT's evaluation of Appendix C will be based on changes in the IT security or regulatory requirements. Changes to Appendix C must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be provided to the Vendor with the understanding that the Vendor will adhere to the most current State IT security policies.

1.42 VENDOR ELECTION NOT TO RENEW CONTRACT OR TO INCREASE FEES:

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

2.0 BIT STANDARD STATE CONTRACT TERMS IF STATE HOSTED

2.1 PRODUCT SUPPORT:

The State will install and operate the Vendor's product on the State's computing infrastructure. The State will not be responsible for added support costs if the Vendor determines that the Vendor is unable to meet the support commitment(s) given by the Vendor in this agreement. Any additional costs for support will be borne by the Vendor.

2.2 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.

2.3 LICENSE TO PERFORM SECURITY SCANNING:

Before acceptance by the State the Vendor will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Vendor or

the Vendor has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Vendor on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Vendor. The State will not be charged for any costs incurred by Vendor in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Vendor.

2.4 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. Vendors 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 or security settings 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.

2.5 SECURE PRODUCT DEVELOPMENT:

By signing this agreement, the Vendor agrees to provide the following information to the State:

A. Name of the person responsible for certifying that all deliverables are secure.
B. Documentation detailing the Vendor's version upgrading process.
C. Notification process for application patches and updates.
D. List of tools used in the software development environment used to verify secure coding.
E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform, including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

At the State's discretion the State will discuss the security controls used by the State with the Vendor upon the Vendor signing a non-disclosure agreement.

2.6 DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION:

During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Vendor will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the 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 shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the 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 and or hardware that meets the State's requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State's satisfaction within thirty (30) days of the denial of access to or

removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the Agreement may be terminated.

2.7 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.

2.8 USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE:

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

2.9 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.

2.10 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.

2.11 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.

2.12 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.

2.13 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.

2.14 USE OF NONSTANDARD TECHNOLOGY:

If any changes involving nonstandard technology need to be made by the Vendor after implementation it must first go through the State's IT Change Management process. The Vendor cannot make any changes before receiving a copy of the change management form approving the exact change the Vendor proposes to make. The State at its discretion, using whatever methodology the State wishes, can scan the technology that is proposed to be changed prior to and after the change. At the State's discretion the Vendor must perform the back-out procedures agreed to in the change management form. If any damages and or loss of functionality of any of the State's systems are the result of the Vendor not getting approval for the change before making it the Vendor will be held financially liable for the costs due to the damage and or loss of functionality of the State's systems. The Vendor is also liable if the Vendor exceeds the authority granted by the State to make the change and it results in damage and or loss of functionality of any of the State's systems. The liability limits elsewhere in this Agreement do not apply in this situation. The Vendor should contact the State Contact to start the change management process. If the change must be

immediate there is an Emergency Change Management process that must be used. It will not be considered an emergency if the change is because of the Vendor's business requirements or needs. If the change is not approved the Vendor may request a meeting to discuss the reasons for the disapproval and present additional information in support of the change. The state will consider the additional reasons and re-review the change request. The state shall not be obligated to make a third review if the second review results in a second disapproval.

3.0 BIT STANDARD STATE CONTRACT TERMS IF VENDOR HOSTED

3.1 PROVISION OF DATA:

Upon notice of termination by either party, the State will be provided by the Vendor all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Vendor with all current State Data in a non-proprietary form. 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.

3.2 DATA LOCATION:

The Vendor shall provide its services to the State as well as storage of State data solely from data centers in the continental United States. The Vendor will not allow any State to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall not allow its employees or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access State data remotely only as required to provide technical support or to fulfill the terms of this Agreement. If the State's data being remotely accessed is legally protected data or considered sensitive by the State, then:

i. The device used must be password protected;
ii. Multifactor Authentication must be used;
iii. The data is encrypted to at least AES 256 both in transit and in storage;
iv. Data is not put onto mobile media;
v. No non-electronic copies are made of the data;
vi. The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed;

The State's Data Sanitization policies are to be followed when the data is no longer needed on the device used to access the data remotely.

3.3 DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State's data at

any time. To this end, the Vendor shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

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

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

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

3.4 INDEPENDENT AUDIT:

The Vendor will disclose any independent audits that are performed on any of its systems. The systems included under this requirement are the Vendor's data center. This information on an independent audit(s)-shall be provided to the State in any event, whether the audit or certification process is successfully completed or not. The audit shall also be disclosed if the audit process did not result in a positive outcome. The Vendor will provide a copy of the findings of the audit(s) to the State.

3.5 NON-DISCLOSURE AND SEPARATION OF DUTIES:

The Vendor shall 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's data or the hardware the State's data resides on.

3.6 BUSINESS CONTINUITY AND DISASTER RECOVERY:

The Vendor shall provide a business continuity and disaster recovery plan upon request and ensure that the State's Recovery Time Objective (RTO) of twelve (12) hours and Recovery Point objective (RPO) of three (3) days is met. For purposes of this contract, a

"Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Vendor's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Vendor as soon as possible after the State deems a service outage to be a Disaster.

3.7 STOLEN DATA LIABILITY:

In no event shall the Vendor be liable for loss of good will, or for special, indirect, incidental, consequential or punitive damages arising from the state's use of the services of the Vendor, regardless of whether such claim arises in tort or in contract.

If the state's records or other data submitted for processing are lost or damaged as a result of any failure by the Vendor, its employees or agents to exercise reasonable care to prevent such loss or damages the Vendor's liability on account of such loss or damages shall not exceed the reasonable cost of reproducing such records or data. This limitation shall not apply in the event that the records or data cannot be reproduced at reasonable cost.

3.8 EXTRACTION OF DATA:

Upon notice of termination by the Vendor or upon reaching the end of the term, any information stored in repositories not hosted on the State's infrastructure shall be extracted in a format to enable to State to load the information onto\into repositories. If this is not possible the information metadata, including data structure descriptions and data dictionary, and data will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State again requires that State applications that store information to repositories not hosted on the State's infrastructure require the Vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. The Vendor recognizes and agrees that the State cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and Vendor.

3.9 FACILITIES INSPECTION:

The Vendor grants authorized State and/or federal personnel access to inspect their systems, facilities, work areas, contractual relationships with third parties involved in supporting any aspects of the hosted system, and the systems that support/protect the hosted system. This access will be granted on 24-hour notice. Such personnel will be limited to staff authorized by the State or the federal government to audit the system, and

representatives of the state entity that funds the hosting. The State accepts that access will be arranged with an escort, and the Vendor commits that the escort will have the access and authority to provide physical access to facilities, answer appropriate questions, and provide requested documentation, including but not limited to executed contract terms, operating procedures, records of drills and tests, evidence of background checks, security logs, and any other items required by State or federal audit requirements or as deemed by the State to be required to demonstrate the Vendor is complying with all contract terms.

3.10 HOST FACILITY PHYSICAL SECURITY:

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the hosted system resides. Any door security system must either be connected to the building's power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Vendor agrees to provide, at the State's request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the State's system.

3.11 REDUNDANT POWER AND COOLING TO ALL HARDWARE:

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate all facilities supporting the application have adequate redundant power and cooling capacity to operate uninterrupted, and without the need to refuel generators, for not less than 24 hours in the event the local external power fails.

3.12 UPS BACKUP:

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate UPS power to carry the systems for not less than 10 minutes, and to protect the system from power fluctuations including, but not limited to, surge, spikes, sags, and instability.

3.13 RIGHTS AND LICENSE IN AND TO STATE DATA:

The parties agree that between them, all rights including all intellectual property rights in and to State's data shall remain the exclusive property of the State, and that the Vendor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. 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.

3.14 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 shall 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.

3.15 SERVICE LEVEL AGREEMENTS:

The Vendor warrants that all services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. The Vendor further warrants that the services will be operational at least 99.99% of the time in any given month during the term of this Agreement. In the event of a service outage, the Vendor will:

A. Promptly and at the Vendor's expense, use commercial best efforts to restore the services as soon as possible, and

B. Unless the outage was caused by a Force Majeure event refund or credit the State, at the State's election, the pro-rated amount of fees corresponding to the time Services were unavailable or $100 US funds per incident, whichever is the greater amount. For the purpose of this agreement, an incident, regardless of time required to return to online position and whether re-keying of data is necessary to return, is defined as any significant reduction in the availability of hosted services lasting more than one minute or resulting in data loss, rework, or occurring more than 3 times in a 24-hour time period. For example, being forced offline no more than twice in 24 hours would not be an incident if the user could get back online within 60 seconds and continue work where he or she left off. Being forced off-line 3 times in a day would be an incident, regardless. Being forced off-line once in a 24-hour period of time, however, that resulted in the user having to rekey data that was lost would be an incident. Entering User authentication to log on shall not be considered data entry.

The Vendor will provide the State with seven days prior notice of scheduled downtime in the provision of services for maintenance or upgrades. To the extent possible, the Vendor will

schedule downtime during times of ordinarily low use by the State. In the event of unscheduled or unforeseen downtime for any reason, except as otherwise prohibited by law, the Vendor will promptly notify the State and respond promptly to the State's reasonable requests for information regarding the downtime.

3.16 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 its response;
C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and
D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

3.17 EDISCOVERY:

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

3.18 DATA RETENTION AND DISPOSAL:

A. Using appropriate and reliable storage media, the Vendor will regularly back up State's data and retain such backup copies for a minimum of 36 months.
B. The Vendor will retain logs associated with End User activity for a minimum of 7 years unless the parties mutually agree to a different period.

3.19 MULTI-TENANT ARCHITECTURE LOGICALLY/PHYSICALLY SEPARATED TO ENSURE DATA SECURITY:

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate safeguards to assure that needed logical and physical separation is in place and enforced to insure data security, physical security, and transport security.

3.20 ACCESS ATTEMPTS:

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 shall be logged by the Vendor. For all systems, the log must include at least: log-in 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, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

3.21 PASSWORD POLICIES:

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

3.22 ANNUAL RISK ANALYSIS:

The Vendor will conduct a risk analysis annually or when there has been a significant system change. The Vendor will provide verification to the State Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

(i) Penetration testing of the Vendor's system.
(ii) Security policies and procedures.
(iii) Disaster recovery plan.
(iv) Security incident plan.
(v) Business Associates Agreements.
(vi) Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the State Contact. The summary will include completion dates for the plan's milestones. Updates on the risk management plan will be sent to the State Contact upon request.

3.23 WEBSITE PERFORMANCE REPORT:

The Vendor will provide to the State reports on the performance of the website being hosted by the Vendor or for the website if hosted by a third party for the Vendor. These reports must be produced by the Vendor on demand. The reports will be in .cvs with a mutually agreed to format and at the State's discretion in an unprocessed format. The metrics in the reports will include i) The total number of visits to the website, ii) The average time the website takes to load, and iii) the average length of time a transaction takes on the website.

3.24 ACCESS TO STATE DATA:

Unless this Agreement is terminated, State access to State data amassed under the project covered by this Agreement will not be hindered if there is a:

i) Contract dispute between the parties to this Agreement.
ii) There is a billing dispute between the parties to this Agreement.
iii) The Vendor merges with or is acquired by another company.

The Vendor will also maintain all security requirements of the State as well as any disaster recovery commitments made under this Agreement.

3.25 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 reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the 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 one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

3.26 SECURING OF DATA:

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the 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. Without limiting the foregoing, the Vendor warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

3.27 SECURITY PROCESSES:

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

3.28 IMPORT AND EXPORT OF DATA:

The State shall 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.

3.29 SYSTEM UPGRADES:

Advance notice of 30 days shall be provided 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 scan can include penetration testing of a test system at the State's discretion.

3.30 PASSWORD PROTECTION:

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

3.31 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.

3.32 MOVEMENT OF PROTECTED STATE DATA:

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

3.33 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.

3.34 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 and/or the Vendor's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

APPENDIX D - Security and Vendor Questions

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. BIT recommends that you utilize your BIT Point of Contact 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.

If you do not know the details of the technologies that vendors 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).

Contractors: 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. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). You will see that these questions are divided into sections to help identify the point of the questions.
Use the last column as needed to explain your answers. Also note that 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 greyed out**. If the contractor answers a question by referencing another document or another part of the RFP response, they must give the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DDC = Data Center; DEV = Development; TEL = Telecommunications; POC = Project Management office

Section A: System Security

The following questions are relevant for all contractors 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	If there is a website that is used by State employees or the public as part of the offeror's solution the website must use SAML or OAUTH2 to provide single-sign-on.				
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?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security 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. Are either of these an issue? If so, please explain.				
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 some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
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?				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 140-2, 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 and/or penetration testing? If yes, how frequency, 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?				
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.				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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/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)?				

#	BIT	Question	Response			
			YES	NO	NA	Explain answer as needed
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 done annually?				
		c. If it is SOC 2 audit report does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				
		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request, a redacted version is acceptable?				
A36		Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
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?				
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B: Hosting

Only for Contractor hosted applications, systems, databases, services and any other technology not hosted on the State's infrastructure. Mark the questions as "NA" if this is an application hosted by the State.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Typically, the State of South Dakota prefers to host all systems. In if the State decides that it would be preferable for the vendor to host the system, is this an option?				
B2	POC	Are there expected periods of time where the application will be unavailable for use?				
B3	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?				
B4	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B5	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?				
B6	DC	Explain your tenant architecture and how tenant data is kept separately?				
B7	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B8	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?				
B9	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?				

#	BIT	Question	Response YES	NO	NA	Explain answer as needed
B10	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?				
B11	DC	How do you secure Internet of Things (IoT) devices on your network?				
B12	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B13	DC TEL	Does your company have an endpoint detection and response policy?				
B14	DC TEL	Does your company have any real-time security auditing processes?				
B15	TELE	How do you perform analysis against the network traffic being transmitted or received by your application, systems and/or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	TELE	How do you monitor your application, systems and/or 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?				
B17	DC TELE	What anti-malware product(s) do you use?				
B18	DC TELE	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?				
B19	DC TELE	Have you ever had a data breach? If so, provide information on the breach.				
B20	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B21	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?				
B22	POC	Will the State of South Dakota own the data created in your hosting environment?				
B23	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

Applies 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**	**Explanation**
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 contractors or third parties engaged in providing this hardware, application or service and pertain to business practices. If the application is hosted by the contractor or the contractor 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 contractor 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?				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 in question?				
		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?				
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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?				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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	TEL DC DEV	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	DC 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?				
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 pertain 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? Please indicate version as appropriate				
		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 and or update roadmap aligns with the release and 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?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
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 so, 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 applications?				
E20	DC	Explain how and where the software validates (e.g., filter with white listing) 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?				
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

Section F: Infrastructure

This pertains 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 as "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
F1	TEL	Is there a workstation install requirement?				
F2	DC	Will the system infrastructure have a special backup requirement?				
F3	DC	Will the system infrastructure have any processes that require scheduling?				
F4	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?				
F5	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?				
F6	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?				
F7	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.				
F8	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.				
F9	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.				
F10	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.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F11	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.				
F12	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.				
F13	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?				
F14	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.				
F15	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				
F16	DC	Will your application require a dedicated environment?				

F17	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F18	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.				

#	BIT	Question	Response			Explain answer as needed
			YES	NO	NA	
F19	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F20	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?				
F21	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. Symantec End Point Protection				
F22	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?				
F23	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?				
F24	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?				
F25	DC TEL	What physical access do you require to work on hardware?				
F26	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

These questions relate 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 the questions 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).				

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
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 services you plan to use located offshore (examples include data hosting, data processing, help desk and 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?				

APPENDIX E - Scanning Permission Form

The offeror acknowledges that the State will be able to do a security scan of the offeror's product or service. This will be a vulnerability scan that will not include a penetration test. The State will use industry standard tools. The State prefers to scan a non-production environment with non-production data. These scans will be done at mutually agreeable times. At the option of the State, a scan that demonstrates that the offeror's product or service meets the State's security requirements can be done either before an agreement between the State and the offeror is signed or after. The offeror should fill in the information below and sign this form authorizing the State to do a security scan. The offeror's employee signing this form must have the authority to commit the offeror to allowing the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. Any RFP response that does not include this signed form will be considered incomplete and may be excluded from further consideration.

Offeror's name: _____

Offeror's security contact's name: _____

Security contact's phone number: _____

Security contact's email address: _____

Web address URL or product name _____ The State will contact the security contact listed above to arrange for a test log in for the scanning.

Offeror's employee acknowledging the right to scan (Print): _____

Title: _____

Date: _____

Signature: _____

APPENDIX F – Security Acknowledgement Form

Please return agreement to your BIT Manager or Designated BIT Contact
All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;

2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;

3. Employee or contractor agrees to follow state and federal regulations in regard to confidentiality and handling of data;

4. Employee or contractor has read and agrees to abide by the Policy;

5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;

6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;

7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;

8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;

9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;

10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);

11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.

Information Technology Security Policy – BIT: **http://intranet.bit.sd.gov/policies/**
Information Technology Security Policy – CLIENT: **http://intranet.bit.sd.gov/policies/**
Information Technology Security Policy – CONTRACTOR: **http://bit.sd.gov/vendor/default.aspx**

Acknowledgement: State of South Dakota Information Technology Security Policy
Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

_____ _____ _____ _____
Employee or Contractor signature Date BIT Manager or Contact Date

_____
Employee or Contractor name and Company name in block capital letters

APPENDIX G – Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT BETWEEN:

THE SOUTH DAKOTA DEPARTMENT OF HEALTH, AND _____ .

This Business Associate Agreement (hereinafter may be referred to as "BAA") is made and entered into by and between the South Dakota Department of Health (hereinafter referred to as "DOH") and _____ (hereinafter referred to as "the vendor"), for the purpose of sharing information between one another regarding medical records of patients to provide for legal, investigative, and other services on behalf of the State of South Dakota.

DOH, and _____ hereby enter into a Business Associate Agreement in consideration of and pursuant to the terms and conditions set forth herein.

1. DOH is a state agency of the State of South Dakota and is governed by the statues and administrative rules of the same.

2. _____ is a private company contracted by DOH to provide and implement the Modifiable Off-The-Shelf Software (MOTS) that serves as the state's medical marijuana patient registry, verification, and medical marijuana business licensing system.

3. This Business Associate Agreement will be effective immediately upon the signing of this document by authorized representatives of all parties.

I. VENDOR RESPONSIBILITIES

_____ is a Business Associate of the Department of Health pursuant to requirements of the Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act §§ 13400-13424, 42 U.S.C. §§ 17921-17954 (2009). State's Administrative Policies and Procedures Statement No. 24, as modified from time to time during the term of this agreement, is incorporated by reference and made a part of this agreement as if fully set forth herein.

I. Privacy and Security Requirements

1. As a Business Associate, the vendor agrees:

a. to use or disclose any Protected Health Information (PHI) solely:
   i. to meet its obligations in this and any other agreements with State;
   ii. as required by applicable law, rule or regulation; and
   iii. as permitted by HIPAA, and any amendments to HIPAA, and subject in particular to limits set forth in 45 CFR § 164.514 (e) (2) (limited data sets) and 45 CFR § 164.502(b) (minimum necessary disclosure requirements);

b. to return or destroy all PHI received from, created, or received on behalf of State, at termination of this agreement, or upon request of the

DOH, whichever occurs first, or, if such return or destruction is not feasible, to extend the protections of this agreement to the information and limit further uses and disclosures of such PHI;

c. to ensure that its agents, including a subcontractor, to whom it provides PHI received from or created by the vendor on behalf of State, agrees to the same restrictions and conditions applicable to the vendor, and agrees to implement reasonable and appropriate safeguards to protect all Electronic Protected Health Information (EPHI). the vendor also agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause a breach of the terms of this agreement;

d. to notify State of any discovery or a breach of unsecured PHI as defined in the HITECH Act or accompanying regulations pursuant to the terms of 45 CFR § 164.410 and cooperate in State's breach analysis procedures, if requested. A breach shall be treated as discovered by the vendor as of the first day on which such breach is known, or, by exercising reasonable diligence, would have been known, and requires notification to State without unreasonable delay and in no event later than thirty (30) calendar days after discovery of the breach. Such notification will contain the elements required in 45 CFR § 164.410; and

e. to comply with all requirements pursuant to the HITECH Act and its implementing regulations, and all additional applicable requirements of the Privacy Rule, including those contained in 45 CFR §§ 164.502(e) and 164.504(e)(1)(ii). The vendor will not directly or indirectly receive remuneration in exchange for any PHI, subject to the exceptions contained in the HITECH Act and without a valid authorization from the applicable individual. The vendor will not engage in any communication which might be deemed to be "marketing" under the HITECH Act, and will comply with all applicable security requirements in 45 CFR §§ 164.308, 164.310, 164.312, and 164.316.

2. Notwithstanding the prohibitions set forth in this agreement, the vendor may use and disclose PHI if necessary, for its proper management and administration or to carry out its legal responsibilities, provided the following requirements are met:

a. the disclosure is required by law; or

b. reasonable assurances are obtained from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. Such person shall notify the vendor of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Availability of PHI

The vendor further agrees:

a. to comply with any request for restrictions on certain disclosures of PHI pursuant to 45 CFR § 164.522, as agreed by State and with notice to the vendor

b. to make PHI available for purposes of accounting of disclosures, as required by 45 CFR § 164.528 and Section 13405(c)(3) of the HITECH Act; and

c. to cooperate in providing any accounting required on a timely basis.

4. Termination
   a. Termination for convenience. Either party may terminate this contract upon 180 days written notice to the other.
   b. Termination for Cause. The vendor authorizes termination of this contract by DOH, If DOH determines that the vendor has violated a material term of the contract.
5. Miscellaneous

a. Vendor agrees to indemnify and hold the State, its officers, agents, and employees, harmless from and against any and all actions, suits, damages, liability, or other proceedings which may arise as the result of performing services hereunder. This section does not require the Vendor to be responsible for or defend against claims or damages arising solely from the errors or omissions of the State, its officers, agents, or employees; or from the errors or omissions of third parties that are not officers, employees or agents of the Vendor, unless such errors or omissions resulted from the acts or omissions of the Vendor. Nothing in this Agreement is intended to impair the insurance coverage of the Vendor or any subrogation rights of the Vendor's insurers.

b. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. The parties agree to take such action as is necessary to amend this Agreement periodically as is necessary to achieve or maintain compliance with the requirements of the HIPAA Rules and any other applicable law.

c. Any reference herein in this Agreement to a federal regulatory section within the Code of Federal Regulations or a HIPAA rule means the section in effect or as subsequently updated, amended, or modified.

d. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA rules.

e. In the event of a conflict in or between the terms of this Business Associate Agreement any interpretation shall ensure compliance with the HIPAA Rules.

f. Any notices hereunder shall be in writing and addressed as follows:

If to the Business Associate/Vendor:

If to Covered Entity/State:

South Dakota Department of Health
Hayes Building
600 East Capitol
Pierre, SD 57501
Attention: _____

In Witness Whereof, the parties signify their agreement by the signatures affixed below.

FOR BUSINESS ASSOCIATE/VENDOR – _____

By: _____ _____
Date

Name:

Title:

FOR COVERED ENTITY/STATE - South Dakota State Department of Health

By: _____ _____
Date

Name:

Title: