State of South Dakota
Master Services Agreement with
Vendor Name

This Master Services Agreement ("MSA") is made and entered into this (Day) day of (Month), 20XX by and between the South Dakota Bureau of Information and Telecommunications, on behalf of the State of South Dakota and its agencies, of 700 Governors Drive, Pierre, SD 57501, (the "State") and (Vendor Name) having a principal office at (Vendor Address) (the "Vendor"). Each party may be referred to as "Party," and both parties may be collectively referred to as "Parties."

This MSA is the result of request for information/proposal process #(RFP Number).

The State hereby enters into this MSA for services with the Vendor in consideration of and pursuant to the terms and conditions set forth in this MSA.

Section I. Scope of Work

A. During the Term of the MSA, the Vendor agrees to provide services to the State of South Dakota and its agencies to (Insert Scope of Work). On an as needed basis, the Vendor may enter into a Statement of Work (SOW) with a state agency to provide services authorized under this MSA. A project's SOW will include the scope of work for that unique project, and it will include additional terms and conditions based upon the unique nature of the project.

B. Additional exhibits within this MSA attached to this MSA and incorporated by reference include:

1. **Attachment A: Certificate of Media Sanitation for Offsite Data**
2. **Attachment B: Information Technology Security Policy – Contractor Version**
3. **Attachment C: Security Acknowledgment Form**

Section II. Term of Agreement

Section III. The "Term of the Agreement" will commence on the date the last signature is applied to this MSA and terminate on (Insert Termination Date), unless sooner terminated pursuant to Section XIV~~Section XI~~V. The Parties will have the option to renew this MSA for (Insert the # of renewals available) additional (Insert the length of those renewal periods)-year periods under the same terms and conditions unless amended by mutual agreement of the Parties pursuant to Section XXXV~~Section~~ XXXV. At a minimum, renewal is contingent upon satisfactory performance of the contract by the Vendor as determined by the State. If the State wishes to renew this MSA, the State will provide a written Request to Renew to the Vendor no less than 90 days prior to the end of the current MSA term. Once a Request to Renew is provided to the Vendor, a written renewal agreement must be executed by the Parties; otherwise this MSA will terminate through expiration of its current MSA term. If the Vendor does not wish to renew this MSA or intends to increase the fees of any SOW, the Vendor must provide the State with 180 days' written notice. The preceding notice requirement is not applicable if the increase in fees was previously negotiated by the Parties.

Section IV. Fees and Payment

The Vendor and the agency in need of services will negotiate fees and payment terms and conditions and incorporate them into each unique SOW. The State or its agencies will not pay the Vendor's expenses as a separate item. Payments will be made pursuant to itemized invoices submitted with a signed state voucher. Payments will be made consistent with SDCL ch. 5-26.

Section V. Employer Identification Number

The Vendor will provide the State with a Certificate of Authority issued from the South Dakota Secretary of State upon execution of this MSA. When the Vendor executes a SOW with a state agency, the Vendor agrees to provide the state agency with its Employer Identification Number, Federal Tax Identification Number, or Social Security Number.

Section VI. Property

When providing services pursuant to a SOW, the Vendor may use some state equipment, supplies, and facilities. The terms and conditions of use of state property or services will be enumerated within a SOW.

Section VII. Indemnification

The Vendor agrees to indemnify and hold the State of South Dakota and its officers, agents, and employees harmless from and against all actions, suits, damages, liability, or other proceedings that may arise as the result of entering into this MSA and any SOW, including but not limited to any claim alleging infringement or any patent, copyright, trade secret, or other intellectual property right. This Section does not require the Vendor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State or its officers, agents, or employees.

Section VIII. Professional Services Quality and Originality Warranties

The Vendor represents and warrants that all professional services provided pursuant to a SOW will be performed in a professional and workmanlike manner. The Vendor further represents and warrants that the deliverables of any SOW will be its own original work, without incorporation of software, text, images, or other assets created by third parties, except to the extent that the State consents to such incorporation in writing.

Section IX. Remedies for Breach of Professional Services Warranties

In the event of a breach of the warranty granted in Section VIII~~Section VII~~ of this MSA, the Vendor, at its own expense, will promptly re-perform the professional services in question. The preceding sentence, in conjunction with the State's right to terminate this MSA and a SOW for breach where applicable, states the State's sole remedy and the Vendor's entire liability for breach of the warrant granted in Section VIII~~Section VII~~.

Section X. Intellectual Property Warranty

The Vendor warrants that it is the owner of the software and services provided pursuant to any SOW entered into pursuant to this MSA, or the recipient of a valid license thereto, and that it has and will

maintain the full power and authority to grant access to the software and services and other rights granted in this MSA and all SOWs without further consent of any third party.

Section XI. Remedies for Breach of Intellectual Property Warranty

In the event of a breach of the warranty granted in Section IX of this MSA, Vendor, at its own expense, will promptly take one of the following actions: (a) secure for the State the right to continue using the technology in question; (b) replace or modify the technology in question to make it non-infringing, provided such modification or replacement will not materially degrade any functionality required by the applicable SOW; or (c) refund the license fee paid for the technology in question for every month remaining in the SOW term following the date after which the State is required to cease operation of the technology. The remedies set forth in the preceding sentence are not exclusive of any others the State may have.

Section XII. Independent Contractor

The Parties are independent contractors and will so represent themselves in all regards. Neither Party is the agent of the other, and either may make commitments on the other's behalf. The Parties agree that no Vendor employee or contractor will be an employee of the State. The Vendor will be responsible for all employment rights and benefits of the Vendor employees, including without limitation: federal, state, and local income and employment taxes and social security contributions; workers' compensation, health benefits, vacation pay, holiday pay, profit sharing, retirement, pension, disability benefits, and other health and welfare benefits, plans, or programs; and insurance.

Section XIII. Reporting

The Vendor agrees to report to the State any event encountered during the Term of the Agreement which results in injury to the person or property of any third party, or which may otherwise subject the Vendor or the State of South Dakota or its officers, agents, or employees to liability. The Vendor will report any such event to the State immediately upon discovery.

The Vendor's obligation under this Section will be to report the occurrence of any event to the State and to make any other report provided for by its duties or applicable law. The Vendor's obligation to report will 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 will not excuse or satisfy any obligation of the Vendor to report any event to law enforcement or other entities under the requirements of any applicable law.

Section XIV. Termination

A. This MSA or any SOW may be terminated by the State upon 30 days written notice.

B. If the Vendor breaches any term or condition of this MSA or any SOW, the State may terminate this MSA or applicable SOW at any time with or without notice. If the State terminates this MSA or a SOW for a breach by the Vendor, any payments due to the Vendor at the time of termination may be adjusted to cover any additional costs to the State as a result of the breach. If the State exercises its right of termination pursuant to this subsection and it is determined that the Vendor was not at fault for the breach or a breach did not occur, the State agrees to pay the Vendor for eligible services rendered and expenses incurred up to the date of termination.

C. Alternatively, the State retains the discretion to provide the Vendor the opportunity to cure a breach of this MSA or applicable SOW. If the State exercises its discretion, the State will provide the Vendor notice of its opportunity to cure the breach. If the breach remains unresolved after three days, the State may require the Vendor to send at least one qualified and knowledgeable representative to the State's site where the system in question is located. The representative will continue to work towards a resolution of the breach. The Vendor will bear all costs associated with curing the breach. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this MSA, the applicable SOW, or by law.

D. Upon termination of this MSA or a SOW, the Vendor acknowledges the State's right to take over the work or may award the work to another party.

Section XV. Confidentiality of Information

A. **Definition:** "Confidential Information" includes all information disclosed by the State to the Vendor, including but not limited to: names, social security numbers, employee numbers, addresses, other data about applicants, employees, and clients to whom the State provides services of any kind, and any other nonpublic, sensitive information disclosed by the State. Notwithstanding the foregoing, Confidential Information does not include information that:
   1. was in the public domain at the time it was disclosed;
   2. was known to the Vendor without restriction at the time of disclosure by the State;
   3. The Vendor received written approval by the State to disclose;
   4. was independently developed by the Vendor without the benefit or influence of the State's information; or
   5. becomes known to the Vendor without restrictions from a source not connected to the State.

B. **Nondisclosure:** The Vendor will not use Confidential Information for any purpose other than to facilitate the transactions contemplated by this MSA or an applicable SOW ("Purpose"). The Vendor will not disclose Confidential Information to:
   1. any employee or contractor of the Vendor unless such person needs access in order to facilitate the Purpose and executes a nondisclosure agreement with the employee or contractor with terms no less restrictive than those of this MSA or an applicable SOW; and
   2. any other third party without the State's prior written consent.

   Without limiting the generality of the foregoing, the Vendor must protect Confidential Information with the same degree of care it sues to protect its own confidential information of similar nature and importance, but with no less than reasonable care. Vendor must promptly notify the State of any misuse or misappropriation of Confidential Information that comes to the Vendor's attention. Notwithstanding the foregoing, the Vendor may disclose Confidential Information as required by applicable law or by proper legal or governmental authority. The Vendor must give the State prompt notice of any such legal or governmental demand and reasonably cooperate with the State in any effort to seek a protective order or otherwise to contest such required disclosure, at the State's expense.

C. **Injunction, Termination, and Retention of Rights:**
   1. *Injunction.* The Vendor agrees that breach of this Section XV would cause the State irreparable injury, for which monetary damages would not provide adequate compensation, and that in addition to any other remedy, the State will be entitled to

injunctive relief against such breach or threatened breach, without proving actual damage or posting a bond or other security.

2. *Return upon Termination.* Upon termination of this MSA or an applicable SOW, the Vendor will return all copies of Confidential Information to the State or certify, in writing, the destruction thereof.
3. *Retention of Rights.* This MSA or an applicable SOW does not transfer ownership of Confidential Information or grant a license thereto. Except to the extent that another section of this MSA or an applicable SOW specifically provides to the contract, the State will retain all right, title, and interest in and to all Confidential Information.

Section XVI. State Data

A. **Definition: "**State Data" is any data produced or provided by the State as well as any data produced or provided for the State by the Vendor or a third party.

B. **Data Location and Offshore Services:** The Vendor must provide its services to the State as well as storage of State Data solely from data centers located in the continental United States. The Vendor will not provide access to State Data to any entity or person(s) located outside the continental United States that are not named in this MSA without prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

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

D. **Remote Access:** The Vendor will prohibit its employees, agents, affiliates, and subcontractors from accessing State Data remotely except as necessary to provide the services under this MSA and any applicable SOW and consistent with all contractual and legal requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication. If the State Data that is being remotely accessed is legally protected data or considered sensitive by the State, then:
   1. the device must be password protected;
   2. the data is not put onto mobile media (such as flash drives);
   3. no non-electronic copies are made of the data;
   4. the Vendor must maintain a log detailing the data which was accessed, when it was accessed, and by whom it was accessed.

E. **Non-Disclosure and Separation of Duties:** The Vendor will enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State Data or the hardware that State Data resides on. The Vendor will limit staff knowledge to those staff whose duties require them to have access to State Data or the hardware State Data resides on.

F. **Securing of Data:** All facilities used to store, and process State Data will employ industry best practices, including appropriate administrative, physical, and technical safeguards to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved.

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

H. **Lost or Damaged Data Liability:** If State Data is lost or damaged as a result of any failure by the Vendor, its employees, or its agents to exercise reasonable care to prevent such loss or damage, then the Vendor's liability will not exceed the reasonable cost of reproducing the lost or damaged data. The Parties agree this limitation of liability will trump any limitation of liability found in a SOW as it relates to lost or damaged State Data.

I. **Rights, Use, and License of and to State Data:** The parties agree that all rights, including all intellectual property rights, in and to State Data will remain the exclusive property of the State. The State grants the Vendor a limited, nonexclusive license to use the State Data solely for the purpose of performing its obligations under this MSA or a SOW. This MSA or SOW 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 MSA or the SOW.

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

   1. The Vendor will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, use, or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information that is confidential under applicable federal, state, or international law, rule, regulation, or ordinance. Such security measures will be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
   2. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this MSA and any SOW.
   3. The Vendor will not use State Data for the Vendor's own benefit and will not engage in data mining of State Data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State Data.

J. **Continued Access to State Data:** The Vendor agrees it will not hinder the State's access to State Data if there is a contract dispute between the Parties, if there is a billing dispute between the Parties, or if the Vendor merges with or is acquired by another entity. In addition, the Vendor must maintain all security requirements and disaster recovery commitments of this MSA and any active SOW during such incidents.

K. **Legal Requests for State Data:** Except as otherwise expressly prohibited by law, the Vendor will:

   1. immediately notify the State of any subpoenas, warrants, or other legal order, demand, or request received by the Vendor seeking State Data maintained by the Vendor;
   2. consult with the State regarding the Vendor's response;
   3. cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the order, demand, or request; and
   4. Upon the State's request, provide the State with a copy of both the order, demand, or request and the Vendor's proposed or actual response to the order, demand, or request.

L. **eDiscovery:** The Vendor will contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to State Data. The Vendor will not respond to service of

process and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

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

N. **Data Sanitization:** At the end of a project covered by a SOW, the Vendor will return all State Data to the State 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 National Institute of Standards and Technology (NIST) Special Publication 800-88. The Vendor must complete and provide to the State point of contact a completed Certificates of Sanitization for Offsite Data, attached to this MSA as Attachment A. 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 method that does satisfy the State. This contract clause remains in effect for as long as the Vendor, and the Vendor's subcontractors, agents, assigns, and affiliated entities have the State Data, even after the MSA or any SOW is terminated or the project is completed.

Section XVII. Security Processes

The Vendor will disclose its non-proprietary security processes and technical limitations to the State so adequate protection and flexibility can be attained between the State and the Vendor, e.g. virus checking and port sniffing.

Section XVIII. Password Policies

Password policies for the Vendor's employees will be documented annually and provided to the State to ensure adequate password protections are in place. Logs and administrative settings will be provided to the State upon request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multi-factor Authentication.

Section XIX. Adverse Event

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

Section XX. Threat Notification

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

Section XXI. Access Attempts

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

Section XXII. Access to Protected Data

For the purposes of this MSA and any SOW, "Protected Data" means data protected by any law, regulation, industry standard, or has been designated as sensitive by the federal or a state government. The Parties agree that if a SOW provides the Vendor access to the State's Protected Data, then the following contract clauses apply to that SOW:

A. **Security Incident Notification:** For purposes of this MSA and any SOW, "Security Incident" is a violation of any Bureau of Information and Telecommunications (BIT) security or privacy policy or contract agreement involving Protected Data or the imminent threat of a violation. The BIT security and privacy policies can be found in the Information Technology Security Policy (ITSP), attached to this MSA and fully incorporated in this MSA as Attachment B. The Vendor will implement, maintain, and update Security Incident procedures that comply with all state standards and federal and state requirements. The Vendor agrees to notify the State of a Security Incident. To the extent probes and reconnaissance scans common to the industry constitute Security Incidents, the Parties agree that this MSA constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State is required. Probes and reconnaissance scans include, but are not limited to, pings and other broadcast attacks on the Vendor's firewall, port scans, and unsuccessful log-on attempts if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by a legal requirement, the Vendor will provide notice of the Security Incident to only the State. The State will determine if notification to the public will be made 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 must approve the content of the information. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

1. The Vender must notify the State point of contact within 12 hours of the Vendor becoming aware that a Security Incident has occurred. If notification to the State is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within 12 hours after law enforcement grants permission for the release of information on the Security Incident.
2. At a minimum, notification of a Security Incident state the nature of the Protected Data exposed, the time the Incident occurred, and a general description of the circumstances of the Incident. If any of the preceding information is not available within the notification time period, the Vendor must provide the State with all available information along with the reason for the incomplete notification. The Vendor must provide the missing information to the State immediately upon the information becoming available.
3. At the State's discretion, within five business days of a Security Incident, the Vendor must provide to the State all data available including: (i) contact information for the Vendor's point of contact for the Incident: (ii) date and time of the Incident; (iii) date and time the Incident was discovered: (iv) description of the Incident including the Protected Data involved, being as specific as possible; (v) the potential number of records or, if unknown, the range of records; (vi) address where the Incident occurred: and, (vii) the nature of the technologies involved. If any of the preceding information is not available within the specified time period, the Vendor must provide the State with all available information along with the reason for the incomplete information. The Vendor must provide the missing information to the State immediately upon the information becoming available.
4. The Vendor is responsible for complying with South Dakota Codified Law Chapter 22-40 when applicable to a Security Incident. This legal requirement does not replace the Vendor's obligations found in the preceding three subsections.

B. **Handling of Security Incident:** At the State's discretion, the Vendor may be required to preserve all evidence regarding a Security Incident including, but not limited to, communications, documents, and logs. In addition, the Vendor will:
   1. fully investigate each Security Incident;
   2. cooperate fully with the State's investigation and analysis of and response to the Security Incident;
   3. make a best effort to implement necessary remedial measure as soon as it is possible; and
   4. document responsive actions taken related to the Incident, including any post-Incident review of events and actions taken to implement changes in business practices in providing the services covered by the applicable SOW.

   If the State determines the Security Incident was due to the actions or inactions of the Vendor, the Vendor must pay for and use a credit monitoring service, call center, forensics company, advisors, or public relations firm to respond to the Incident; all of which services must be preapproved by the State. The State may require the Vendor to offer and pay for one year 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 of the Vendor, which the Vendor will pay for. If the State requires a risk assessment, the State will mandate the methodology and the scope of the assessment. The State reserves the right to select a third party to conduct the risk assessment.

   If the Vendor is required by federal, state, or international law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be

reported to the State within 12 hours of the investigation report being completed. If the Vendor is required by federal, state, or international law or regulation to notify the affected parties, the State must also be notified unless otherwise prohibited by law.

Notwithstanding any other provision of this MSA or any SOW, 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 for investigating and remediating a Security Incident including, but not limited to, providing notification to regulatory agencies or other entities as required by law or contract. The Vendor will pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

C. **Security Acknowledgment Form:** The Vendor must sign the Security Acknowledgement Form, which is attached to this MSA as Attachment C. Before work on a SOW may begin, the signed Security Acknowledgement form must be approved by BIT and the approval must communicated to the Vendor. This form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor and its employees and subcontractors participating in the work will abide by the policies found within the ITSP. Failure to abide by the requirements of the ITSP or the Security Acknowledgement form is considered a breach of this MSA and any applicable SOW. The Vendor is required to submit a new signed Security Acknowledgment Form when a new employee or subcontractor begins work on the project after the original Form is approved by the State; failure to do is a breach of this MSA and applicable SOW. The State reserves the right to require the removal of an employee or subcontractor from the project covered by a SOW if that employee or subcontractor violated any requirement of the ITSP.

D. **Background Investigations:** The State requires any person who is fulfilling the Vendor's obligations under this MSA and an appliable SOW and who writes or modifies state-owned software, alters hardware, configures software of state-owned technology resources, has access to source code or Protected Data, or has access to secure areas to undergo a fingerprint-based background investigation. The fingerprints will be used to check the criminal history records of both the State of South Dakota and the Federal Bureau of Investigation. These background investigations will be performed by the State with support from the State's law enforcement agencies. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two to four weeks to complete this process. If work assignments change after the initiation of the project covered by an applicable SOW so that a new person will be fulfilling the Vendor's obligations for the project and that person will be writing or modifying State owned software, altering hardware, configuring software of state-owned technology resources, have access to source code or Protected Data, or have access to secure areas then a background investigation must be performed on that new person. The State reserves the right to require the Vendor to prohibit any person fulfilling the Vendor's obligations from performing work under an applicable SOW whenever the State, in its sole discretion, believes that having that specific person perform work under the SOW is detrimental to the project or is considered by the State to be a security risk based on the results of the background investigation. The State will provide the Consultant with notice of this determination.

E. **Restriction on Use of Protected Data in a Non-Production Environment:** The Vendor cannot use Protected Data in a non-production environment. Any non-production environment that is found to have Protected Data must be purged immediately and the Vendor must immediately notify the State point of contact. Upon receipt of notice, the

State will determine if such an event qualifies as a Security Incident. Protected Data that is de-identified, aggregated, or hashed is no longer considered to be Protected Data.

F. **Movement of Protected Data:** All Protected Data must be kept secure. When Protected Data is moved to any of the Vendor's production systems, security must be maintained. The Vendor will ensure that the Protected Data will at least have the same level of security as it had in the State's environment, the policies for which are found in the ITSP.

Section XXIII. Multi-factor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor's subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used 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.

Section XXIV. Training Requirements

All persons fulfilling the Vendor's obligations under this MSA and any SOW must successfully complete a cyber-security training program at the time of hire and annually thereafter. The training must include, but is not limited to: legal requirements for handling data, media sanitation, strong password protection, 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, and security incident response.

Section XXV. Rejection or Ejection of Vendor

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

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

Section XXVI. Service Bureau

Consistent with use limitations specified in the MSA, 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.

Section XXVII. Software Functionality and Replacement

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

The Vendor agrees that:

A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.
B. If, in the opinion of the State, the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State will have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

Section XXVIII. Federal Intellectual Property Bankruptcy Protection Act

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

Section XXIX. Cessation of Business

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

Section XXX. Annual Risk Assessment

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

A. Penetration testing of the Vendor's system;
B. Security policies and procedures;
C. Disaster recovery plan;
D. Business Associate Agreements; and

E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

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

Section XXXI. Independent Audit

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

Section XXXII. Service Level Agreements

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

Section XXXIII. Funding Out

This MSA and all SOWs depend 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 MSA or the applicable SOW will be terminated by the State. Termination pursuant to this Section is not a default by the State nor does it give rise to a claim against the State.

Section XXXIV. Assignment

This MSA and any SOW may not be assigned without the express prior written consent of the State.

Section XXXV. Amendment

This MSA or any SOW may not be amended except in writing, which writing will be expressly identified as a part of this MSA or the applicable SOW and be signed by the authorized representatives of both Parties.

Section XXXVI. Change Management Process

The Parties may agree to modify the services provided pursuant to a SOW through a written change order specifically referencing both this MSA and the applicable SOW. Such change order will become effective and part of the applicable SOW when executed by both parties, containing

the dated signatures of authorized representatives of the Parties. The services described within the change order will become part of the applicable SOW deliverables.

Section XXXVII. Governing Law

This MSA and all SOWs will be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. The venue for any lawsuit pertaining to or affecting this MSA and all SOWs will be in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota**.**

Section XXXVIII. Insurance

At all times during the Term of the Agreement, the Vendor will obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. **Commercial General Liability Insurance:** The Vendor will 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 will apply separately to this MSA or a SOW or be no less than two times the occurrence limit.

B. **Professional Liability Insurance or Miscellaneous Professional Liability Insurance:** The Vendor will maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1 million.

C. **Business Automobile Liability Insurance:** The Vendor will maintain business automobile liability insurance or equivalent form with a limit of not less than $1 million for each accident. Such insurance will include coverage for owned, hired, and non-owned vehicles.

D. **Workers' Compensation Insurance:** The Vendor will maintain workers' compensation and employer's liability insurance as required by South Dakota law.

E. **Cyber Liability Insurance:** The Vendor will maintain cyber liability insurance with liability limits in the amount of $3 million to protect any and all State Data the Vendor receives as part of the project covered by this MSA or any SOW 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 MSA or any SOW, then the Vendor will include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State Data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance will cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this MSA or any SOW, the Vendor will furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this MSA or any SOW and which provide that such insurance may not be canceled, except

on 30 days prior written notice to the State. The Vendor will furnish copies of insurance policies if requested by the State. The insurance will stay in effect for three years after the work covered by this MSA or any SOW is completed.

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

Section XXXIX. Compliance

The Vendor will comply with all federal, international, state, and local laws, regulations, ordinances, guidelines, permits, and requirements applicable to providing services pursuant to this MSA and all SOWs, and will be solely responsible for obtaining current information on such requirements. Liability resulting from noncompliance with applicable standards required by federal, international, state, and local laws, regulations, ordinances, guidelines, permits, and other requirements is assumed entirely by the Vendor.

Section XL. Subcontractors

The Vendor may not use subcontractors to perform services described in any SOW without the express written consent of the State. The Vendor will include provisions in its subcontracts requiring the subcontractors to comply with the applicable provisions of this MSA and the applicable SOW, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this MSA. The Vendor will require its subcontractors, agents, and employees to comply with applicable federal, state, and local laws, regulations, ordinances, guidelines, permits, and requirements. The Vendor will adopt review and inspection procedures as are necessary to ensure such compliance.

Section XLI. Work Product and Ownership and Use

The Vendor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, agreements, Confidential Information, State data, Protected Data, any information discovered by the State, PII, data protected under FERPA, PHI, 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 MSA and all SOWs will 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.

Papers, reports, forms, or other material which are a part of the work under this MSA or any SOW will not be copyrighted without written approval of the State. If any copyright does not fully belong to the State, the State reserves a royalty-free, non-exclusive, non-transferable, and irrevocable license to reproduce, publish, and otherwise use and to authorize others to use on the State's behalf any such work for government purposes.

Section XLII. Notice

Any notice or other communication required under this MSA will be in writing and sent to the address set forth above. For this MSA, notices will be given by and to **(Insert BIT POC for MSA), South Dakota Bureau of Information and Telecommunications,** on behalf of the State, and by **(Name of Vendor POC), (Vendor POC Title), (Vendor Company Name)**, on behalf of the Vendor, or such authorized designees as either party may from time to time designate in writing. The Parties acknowledge and agree that each unique SOW will designate an agency specific point of contact to whom notices must be given to.

Notices or communications to or between the Parties will be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination must be sent by registered or certified mail, or, if personally delivered, when received by such party. Notices or communications to or between the parties by email will be deemed to have been delivered when sent by the sending party.

Section XLIII. Electronic Signature

The Parties agrees that this MSA and any SOW may be electronically signed, and that any electronic signatures appearing on this MSA or a SOW are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility.

Section XLIV. Severability

In the event that any court of competent jurisdiction rules any provision of this MSA or a SOW unenforceable or invalid, such ruling will not invalidate or render unenforceable any other provision hereof.

Section XLV. Entire Agreement

This MSA sets forth the entire agreement of the Parties and supersedes all prior or contemporaneous writings, negotiations, and discussions with respect to its subject matter. Neither Party has relied upon any such prior or contemporaneous communications.

Section XLVI. State of Israel

By signing this MSA, the Vendor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of the contract, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott 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 terminate this MSA. During the term of this MSA, if the Vendor no longer complies with this certification, the Vendor agrees to provide immediate written notice to the State and agrees such noncompliance may be grounds for termination of this MSA and any active SOW.

Section XLVII. Conflict of Interest

The Vendor agrees to establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal organizational conflict of interest,

or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Vendor expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

Section XLVIII. Browser

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

Section XLIX. Information Technology Standards

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

Section L. 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 MSA or any SOW unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

Section LI. 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 MSA or any SOW. Any additional costs for support will be borne by the Vendor.

Section LII. Security

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

By signing this MSA and any SOW, the Vendor warrants that:

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

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

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

B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

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

Section LIV. Malicious Code

A. The Vendor warrants that the MSA and any SOW deliverables contain no code that does not support an application requirement.
B. The Vendor warrants that the MSA and any SOW deliverables contains no malicious code.
C. The Vendor warrants that the Vendor will not insert into the MSA and any SOW deliverables or any media on which the MSA and any SOW deliverables is delivered any malicious or intentionally destructive code.
D. In the event any malicious code is discovered in the MSA and any SOW deliverables, the Vendor must provide the State at no charge with a copy of or access to the applicable MSA and any SOW deliverables that contains no malicious code or otherwise correct the

affected portion of the services provided to the State. The remedies in this Section are in addition to other additional remedies available to the State.

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

During the life of this MSA and any SOW the application and hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the State determines are unacceptable results.

The Vendor will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application or hardware. At the discretion of the State, contractual payments may be suspended while the application or hardware is denied access to or removed from production. The reasons can be because of the Vendor's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval.

It is expected that the Vendor will provide the State with proof of the safety and effectiveness of the remedy, update, or patch proposed before the State provides access to the production system. The State will sign a non-disclosure agreement with the Vendor if revealing the update or patch will put the Vendor's intellectual property at risk. If the remedy, update, or patch the Vendor proposes is unable to present software or hardware that meets the State's requirements, as defined by the State, which may include but is not limited to security, functionality, or unsupported third party technologies, to the State's satisfaction within 30 days of the denial of access to or removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same 30 days then at the State's discretion the MSA or SOW may be terminated.

Section LVI. 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 MSA. 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 MSA or any SOW. All such movement of product can be done by the State without any additional fees or charges by the Vendor.

Section LVII. Use of Product on Virtualized Infrastructure and Changes to that Infrastructure

The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its

hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product will be the only consideration in licensing compliance related to computing resource capacity.

Section LVIII. Load Balancing

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

Section LIX. Backup Copies

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

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

Section LX. Use of Abstraction Technologies

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

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

Section LXI. Scope of Use

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

Section LXII. Application Programming interface

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

Section LXIII. License Agreements

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

Section LXIV. Web and Mobile Applications

A. The Vendor's application is required to:

1. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State,
7. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,
11. access no data outside what is defined in the "About" information for the Vendor's application,
12. have Single Sign On capabilities with the State's identity provider, and
13. any application to be used on a mobile device must be password protected.

B. The Vendor is required to disclose all:

1. functionality,
2. device and functional dependencies,
3. third party libraries used,
4. methods user data is being stored, processed, or transmitted,

5. methods used to notify the user how their data is being stored, processed, or transmitted,
6. positive actions required by the user to give permission for their data to be stored, processed and or transmitted,
7. methods used to record the user's response(s) to the notification that their data is being stored, processed, or transmitted,
8. methods used to secure the data in storage, processing, or transmission,
9. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits,
10. methods used to create and customize existing reports,
11. methods used to integrate with external data sources,
12. methods used if integrates with public cloud provider,
13. methods and techniques used and the security features that protect data, if a public cloud provider is used, and
14. formats the data and information uses.

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

Section LXV. 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.

Section LXVI. Use of Nonstandard Technology

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.

If any changes involving nonstandard technology need to be made by the Vendor after implementation the changes 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 MSA 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 will not be obligated to make a third review if the second review results in a second disapproval.

Section LXVII. Internet of Things (IoT)

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

Section LXVIII. Banned Hardware and Software

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

Section LXIX. Hardware Passwords

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

Section LXX. Third Party Hosting

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

Section LXXI. Import and Export of Data

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

Section LXXII. System Upgrades

The Vendor must provide advance notice of 30 days to the State of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software, or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scans can include penetration testing of a test system at the State's discretion.

Section LXXIII. Banned Services

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

Section LXXIV. Certification Relating to Prohibited Entity

Pursuant to South Dakota Executive Order 2023-02, by entering into this MSA with the State of South Dakota, the Vendor certifies and warrants that the Vendor is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02.

The Vendor agrees that if this certification is false, the State may terminate this MSA with no further liability to the State. The Vendor further agrees to provide immediate written notice to the State if during the term of the MSA it no longer complies with this certification, and the Vendor agrees such noncompliance may be grounds for contract termination.

Section LXXV. Conflicts among Attachments

In the event of conflict with an attachment to this MSA, this main body of this MSA will govern. In addition, no SOW or other attachment incorporated into this SOW or other attachment incorporated into this MSA after execution of this main body of this MSA will be construed to amend this main body unless it specifically states its intent to do so and cites the section or sections amended.