

STATE OF NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY	INVITATION FOR BIDS NO. IFB-41-DIT-1512215188 – SITP 900121
	Offers will be publicly opened: April 2, 2025, at 2:00PM EST
	Issue Date: March 14, 2025
Refer <u>ALL</u> inquiries regarding this IFB to: <i>The procurement lead (Belinda Edwards) through the Ariba Sourcing Tool Message Board</i>	Commodity Number: 811620
	Description of Solicitation: ESRMO Identity Governance Administration-Zilla Tool
	Using Agency: NCDIT
See page 2 for mailing instructions.	Requisition No.: RQ182458

OFFER AND ACCEPTANCE

The State seeks offers for the Software, Services and/or goods described in this solicitation. The State's acceptance of any offer must be demonstrated by execution of the acceptance found below and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: In cases of conflict between documents comprising the contract, the order of precedence shall be (1) Best and Final Offers, if any, (2) special terms and conditions specific to this IFB, (3) specifications, (4) Department of Information Technology Terms and Conditions of this IFB, and (5) the agreed portions of the awarded Vendor's offer. **No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the contract.**

EXECUTION

In compliance with this IFB and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein. By executing this offer, I certify that this offer is submitted competitively and without collusion.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

VENDOR:		
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY, STATE & ZIP:	TELEPHONE NUMBER:	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING:	FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:

Offer valid for sixty (60) days from date of offer opening unless otherwise stated here: ____ days

ACCEPTANCE OF OFFER

If any or all parts of this IFB are accepted, an authorized representative of Department of Information Technology shall affix their signature hereto. A copy of this acceptance will be forwarded to the successful vendor(s).

<u>FOR STATE USE ONLY</u> Offer accepted and contract awarded _____, as indicated on attached certification, by _____ (Authorized representative of Department of Information Technology).
--

TABLE OF CONTENTS

1.0	INTENT, USE, DURATION AND SCOPE	3
2.0	GENERAL INFORMATION	3
2.1.	VENDOR QUESTIONS.....	3
2.2.	ADDENDA	3
2.3.	OFFER SUBMITTAL AND SCHEDULE	4
2.4.	BASIS FOR REJECTION	5
2.5.	LATE OFFERS.....	5
2.6.	NON-RESPONSIVE OFFERS	6
2.7.	NOTICE TO VENDOR(S).....	6
2.8.	E-PROCUREMENT SOLICITATION.....	6
2.9.	DISTRIBUTORS AND RESELLERS	6
2.10.	POSSESSION AND REVIEW	6
2.11.	BEST AND FINAL OFFERS (BAFO).....	7
2.12.	AWARD.....	7
2.13.	POINTS OF CONTACT.....	7
3.0	SPECIFICATIONS	7
3.1.	VENDOR STANDARD AGREEMENT(S)	7
3.2.	VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.	8
3.3.	E-VERIFY	8
3.4	BRAND SPECIFIC PRODUCT.....	8
3.5.	SECURITY SPECIFICATIONS	8
3.6	ENTERPRISE ARCHITECTURE SPECIFICATIONS	9
3.7	SPECIFICATIONS	11
	Zilla Compliance specifications are as follows:.....	11
3.8.	DELIVERY	11
3.9.	CONTRACT TERM.....	11
4.0	FURNISH AND DELIVER	11
5.0	HISTORICALLY UNDERUTILIZED BUSINESSES	12
6.0	DEPARTMENT OF INFORMATION TECHNOLOGY INSTRUCTIONS TO VENDORS	13
7.0	DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS	15
	ATTACHMENT A – AI or GEN AI ASSESSMENT	30

1.0 INTENT, USE, DURATION AND SCOPE

The purpose of this Invitation for Bid is to obtain pricing for and procure the Identity Governance and Administration (IGA) Zilla Security's Compliance solution to meet the requirements of the NC Statewide Information Security Manual, AC-1, AC-2 as well as other regulatory requirements (IRS, etc.). This IGA solution supports import of data from a variety of sources utilizing standard protocols/APIs for the source where possible, supports import from APIs that can be configured and customized where there is no pre-configured connector, supports import by reading and collecting data from a web page where there is no API option, and supports Comma Separated Value (CSV) file imports. The IGA solution is not dependent upon any specific IAM, PAM, PIM, or PUM solution to obtain data. Review periods for managers and application owners can be conducted against specified criteria such as, but not limited to, account level of access and where an account has access. Reporting on review progress, outcomes of a review set, and broken out by team, reviewee, and/or application is supported. It additionally supports collecting data from internal sources without the need to expose those sources by utilizing collector-type software installed on a system within the State network. Goods and Services will be provided in accordance with the terms and conditions of this IFB.

2.0 GENERAL INFORMATION

2.1. VENDOR QUESTIONS

Vendors must submit questions regarding the IFB no later than **2:00 PM EST March 21, 2025**. Necessary replies will be issued to all Vendors of record as addenda and shall become part of the contract documents. Oral instructions do not form a part of the IFB documents. Vendors will enter "**Questions Solicitation IFB-41-DIT-1512215188**" as the subject of the message.

Questions related to the content of the solicitation, or the procurement process **must** be directed to the person on the title page of this document via the **Sourcing Tool's Message Board** by the date and time specified in the PROCUREMENT SCHEDULE Section of this IFB. No information, instruction or advice provided orally or informally by any State personnel, whether made in response to a question or otherwise in connection with this IFB, shall be considered authoritative or binding. Vendors shall rely *only* on written material contained in the IFB and an addendum to this IFB.

Questions or issues related to using the Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM ET to 5:00 PM ET.

For training on how to use the Sourcing Tool to view solicitations, submit questions, develop responses, upload documents, and submit offers to the State, Vendors should go to the following site: <https://eprocurement.nc.gov/training/vendor-training>.

2.2. ADDENDA

The State may issue addenda if Vendor questions are permitted as described above, or if additional terms, specifications, or other changes necessary for this procurement. All addenda s addenda and shall become part of the contract documents.

2.3. **OFFER SUBMITTAL AND SCHEDULE**

PROCUREMENT SCHEDULE:

IFB Issued	Friday, March 14, 2025
Last Date for Receipt of Questions	Friday, March 21, 2025, 2:00 p.m. EST
Addendum Posting Date	Tuesday, March 25, 2025
Bid Opening Date	Wednesday, April 3, 2025, 2:00 p.m. EST
Anticipated Award Date	Tuesday, April 15, 2025

Microsoft Teams [Need help?](#)

Join the meeting now

Meeting ID: 247 883 211 865

Passcode: nc6m5UV9

Dial in by phone

[+1 984-204-1487,,863404428#](#) United States, Raleigh

[Find a local number](#)

Phone conference ID: 863 404 428#

Join on a video conferencing device

Tenant key: ncgov@m.webex.com

Video ID: 117 465 593 1

[More info](#)

For organizers: [Meeting options](#) | [Reset dial-in PIN](#)

IMPORTANT NOTE: It is the Vendor's sole responsibility to upload their offer to the Sourcing Module by the specified time and date of opening. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues. Vendors must include all the pages of this solicitation in their response.

Tips for Using the Sourcing Tool

1. Vendors should review available training and confirm that they are able to access the Sourcing Event, enter responses, and upload files well in advance of the date and time response are due to allow sufficient time to seek assistance from the North Carolina eProcurement Help Desk.
2. Vendors may submit their responses early to make sure there are no issues, and then submit a revised response any time prior to the response due date and time. The State will only review the most recent response.
3. Vendors should respond to all relevant sections of the Sourcing Event. Certain questions or items are required in order to submit a response and are denoted with an asterisk. The Sourcing Tool will not allow a response to be submitted unless all required items are completed. The Sourcing Tool will provide error messages to help identify any required information that is missing when response is submitted.
4. Simply saving your response in the Sourcing Tool is not the same as submitting your response to the State. Vendors should make sure they complete the submission process and receive a message that their response was successfully submitted.
5. **Only Bids submitted through the Content Section of the Ariba Sourcing Event will be considered. Bids submitted through the Message Board will not be accepted or considered for award.**

If confidential and proprietary information is included in the quote, also submit one (1) signed, REDACTED copy of the quote. Such information may include trade secrets defined by N.C. Gen. Stat. § 66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132- 1.2. Vendor may designate information, Products, Services, or appropriate portions of its response as confidential, consistent with and to the extent permitted under the statutes and rules set forth above. By redacting any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions determined to be confidential and proprietary and redacted as such, meet the requirements of the Rules and Statutes set forth above. However, under no circumstances shall price information be designated as confidential.

If the Vendor does not provide a redacted version of the quote with its bid submission, the Department may release an unredacted version if a record request is received.

2.4. BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed requirement is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State. Vendor contact regarding this IFB with anyone other than NCDIT may be grounds for rejection of said Vendor's offer.

2.5. LATE OFFERS

Regardless of cause, late offers will not be accepted and will automatically be disqualified from further consideration. It shall be the Vendor's sole risk to ensure delivery at the designated office by the designated time. Late offers will not be opened and may be returned to the Vendor at the expense of the Vendor or destroyed if requested.

2.6. NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- “This offer does not constitute a binding offer”,
- “This offer will be valid only if this offer is selected as a finalist or in the competitive range”,
- “Vendor does not commit or bind itself to any terms and conditions by this submission”,
- “This document and all associated documents are non-binding and shall be used for discussion purposes only”,
- “This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties”, or
- A statement of similar intent.

2.7. NOTICE TO VENDOR(S)

The State objects to and will not be required to evaluate or consider any additional terms and conditions not previously agreed to by the State and submitted with an Vendor’s response. This applies to any language appearing in or attached to the document as part of the Vendor’s response. By execution and delivery of this IFB and response(s), the Vendor agrees that any additional terms and conditions, whether submitted purposely or inadvertently, shall have no force or effect.

2.8. E-PROCUREMENT SOLICITATION

This is an E-Procurement solicitation.

- a) General information on the E-Procurement service can be found at <http://eprocurement.nc.gov/>
- b) Within two days after notification of award of a contract, vendor must register in NC E-Procurement @ Your Service at the following web site: <https://vendor.ncgov.com/vendor/login>
- c) As of the IFB submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this IFB.

2.9. DISTRIBUTORS AND RESELLERS

“Resellers” as used herein, refers to businesses that routinely sell or distribute Vendor’s Products, and may include “Distributors”, “Value Added Resellers” (VARs), “Original Equipment Manufacturers” (OEMs), Channel Partners, or such other designations. These businesses must be approved by the State prior to placement of any orders. Any contract established will be subject to this solicitation and any resulting Agreement(s), and to the terms and conditions of the State’s competitive bidding process.

The Agency acknowledges that the Reseller has merely purchased the Third-Party Items for resale or license to the Agency, and that the proprietary and intellectual property rights to the Third-Party Items are owned by parties other than the Reseller (“Third Parties”). The Agency further acknowledges that except for the payment to the Reseller for the Third-Party Items, all of its rights and obligations with respect thereto flow from and to the Third Parties. The Reseller shall provide the Agency with copies of all documentation and warranties for the Third-Party Items which are provided to the Reseller. The Reseller shall assign all applicable third-party warranties for Deliverables to the Agency.

2.10. POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, and to the committee responsible for participating in the evaluation. Vendors who attempt to gain this privileged information, or to influence the evaluation process (i.e. assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 **must be clearly marked as such in the offer when submitted.**

2.11. **BEST AND FINAL OFFERS (BAFO)**

The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendor(s) within this range, e.g. "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers to determine the final rankings.

2.12. **AWARD**

It is the general intent to award this contract to one Vendor. As provided by statute, the award will be based on Best Value Analysis, Lowest Price Technically Acceptable Source Selection Method in accordance with 09 NCAC 06B. 0302 Information Technology Procurement.

The State has implemented the electronic Vendor Portal (eVP) that allow the public to retrieve award notices and information on the Internet at <https://evp.nc.gov>. <https://www.ips.state.nc.us/ips/> Results may be found by searching by Solicitation Number or agency name. This information may not be available for several weeks depending upon the complexity of the acquisition and the length of time to complete the evaluation process.

2.13. **POINTS OF CONTACT**

Contact by the Vendor with the persons shown below for contractual and technical matters related to this IFB is only permitted if expressly agreed to by the purchasing lead named on page 1, or upon award of contract:

Vendor Contractual Point of Contact	Vendor Technical Point of Contact
<p>[NAME OF VENDOR]</p> <p>Street: [STREET ADDRESS]</p> <p>[CITY, STATE, ZIP]</p> <p>Attn: Assigned Contract Manager</p>	<p>[NAME OF VENDOR]</p> <p>Street: [STREET ADDRESS]</p> <p>[CITY, STATE, ZIP]</p> <p>Attn: Assigned Technical Lead</p>

3.0 **SPECIFICATIONS**

3.1. **VENDOR STANDARD AGREEMENT(S)**

The terms and conditions of Vendor's standard license, maintenance or other agreement(s) applicable to Software and other Products acquired under this Agreement may apply to the extent such terms and conditions do not materially change the terms and conditions of this Agreement. In the event of any conflict between the terms and conditions of this Agreement and the Vendor's standard agreement(s), the terms and conditions of this Agreement relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the Terms and Conditions herein shall apply in all cases and supersede any provisions contained in Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns; nor arbitrate any dispute, nor pay late fees, legal fees or other similar costs.

3.2. VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.

In accordance with N.C.G.S. §143B-1361(b), Vendor must detail in the IFB response, the manner in which it intends to utilize resources or workers located outside the U.S. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer. The Vendor shall provide the following for any offer or actual utilization or contract performance:

- a) The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the contract and whether any of this work will be performed outside the United States.
- b) The corporate structure and location of corporate employees and activities of the Vendors, its affiliates or any other subcontractors.
- c) Notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States.
- d) Any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided.

Will any work under this contract be performed outside the United States? ☐ YES ☐ NO

If Vendor answered "YES" above, list the location(s) outside the United States where work under this contract will be performed by Vendor, any sub-contractors, employees, or other persons performing work under the contract.

3.3. E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

3.4 BRAND SPECIFIC PRODUCT

Manufacturer(s) name and product descriptions used in this solicitation are product specific. The items offered in response to this solicitation must be the manufacturer and type specified. Failure to comply with this requirement will result in rejection of offer.

3.5. SECURITY SPECIFICATIONS

3.5.1 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The OSA Data Analytics platform will be required to receive and securely manage data that is classified as High Risk and Program Critical. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding data classification. The policy is located at the following website: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solution which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

Refer to: <https://it.nc.gov/documents/statewide-glossary-information-technology-terms> for descriptions of the Application Criticality categories.

Refer to: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf> [PAT1] for descriptions of NIST system confidentiality, integrity, and availability categories.

- (a) Vendors should provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission and/or prior to award. This report is located at the following website: <https://it.nc.gov/documents/vendor-readiness-assessment-report>
- (b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.
- (i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).
 - (ii) A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.
 - (iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.
- (b) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide additional security documentation upon request by the State during the term of the contract.

Vendors should review, complete and submit with their offer the AI Questionnaire in **ATTACHMENT A**.

3.6 ENTERPRISE ARCHITECTURE SPECIFICATIONS

3.6.1 ARCHITECTURE DIAGRAMS

The two diagrams are Network Architecture and Technology Stack. The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. Details on these diagrams can be found at the following link: <https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192>

The provision of these two diagrams should be supplied at offer submission and/or prior to award.

There may be additional architectural diagrams requested of the vendor after contract award. This will be communicated to the vendor by the agency as needed during the project.

3.6.2 SOLUTION ROADMAP

A Solution Roadmap defines the vision and strategic elements of the solution. The Solution Roadmap is a plan of action for how a Solution will evolve over time. The minimum content should include:

- Vision for the solution

- High-level functionality expected for each solution release into production environment
- High-level timeline
- Description of how customer feedback is collected and incorporated into solution enhancements

Describe the solution roadmap for your product. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned.

3.6.3 IDENTITY AND ACCESS MANAGEMENT

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link: <https://it.nc.gov/services/vendor-engagement-resources#Tab-IdentityAccessManagement-1241>

Describe how your solution supports the above protocols, as well as making them available for application integration/consumption.

3.6.4 INTEGRATION APPROACH

Describe proposed solution capabilities to interoperate with other solutions. Identify the standards supported, integrations platforms, adaptors, APIs, and the like.

3.6.5 DISASTER RECOVERY AND BUSINESS CONTINUITY

Describe the proposed solution capabilities related to the following areas:

Disaster Recovery Plan (DRP) – describe how proposed solution supports Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) metrics.

System Backup – describe backup plan capabilities.

Disaster Recovery Testing – describe the frequency and test procedures for end-to-end disaster recovery testing. Business Continuity Plan (BCP) – describe capabilities proposed solution can provide in support of agency's continuity of operations and incident responses.

3.6.6 DATA MIGRATION

Describe approaches available for data conversion and/or data migration to load current data into proposed solution.

3.6.7 APPLICATION MANAGEMENT

Describe how the proposed solution monitors and reports the metrics on system performance.

Describe how the proposed solution manages user administration.

Describe the audit capabilities of proposed solution related to management of the application.

3.6.8 ACCESSIBILITY

Describe how the proposed solution complies with industry accessibility standards.

Provide product documentation that demonstrates how the proposed solution is digitally accessible or if not fully accessible, provide the roadmap with timeline for remediation.

Standards include:

- W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: <https://www.w3.org/TR/WCAG21/>
- Section 508: <https://www.section508.gov/>
- Voluntary Product Accessibility Template (VPAT®): <https://www.itic.org/policy/accessibility/vpat>

3.7 SPECIFICATIONS

Zilla Compliance specifications are as follows:

- Number of Expected personnel with accounts (e.g. people records): 1000
- Expected data sources (current and future): 25
- Expected NC data source applications (current and future): NCID, AD, Azure Active Directory, RACF, Cisco ISE, PremSys (Badge System), Tenable Security Center Plus, ServiceNow, Touchdown, Ariba, Adobe Sign, DocuSign, AWS, Google Cloud, Azure Cloud, CrowdStrike, Tanium, KnowBe4, M365, Power BI, In-Tune

Connectivity requirements to data sources:

- Internal to the State network: Vendor to provide virtual appliance or container (e.g “Post Office”) that can be run on Red Hat Enterprise Linux 9 within the State network. Appliance/container application shall only make outbound connections to Vendor owned FQDNs or IP addresses.
- Cloud Based: Vendor’s appliance/container shall only connect to Vendor owned FQDNs or IP addresses.

Note: Vendor owned in this case shall mean that the Vendor owns or is otherwise exclusively assigned to use the FQDNs or IP addresses in connectivity scope.

3.8. DELIVERY

Successful Vendor will complete supply of the scope of work within 30 consecutive calendar days after receipt of purchase order either electronically or to the following location(s):

If circumstances beyond the control of the contractor result in a late delivery [or installation], it is the responsibility and obligation of the contractor to notify the Purchasing Agent listed on the purchase order, in writing, immediately upon determining the delay of shipment. The written notification should indicate the anticipated delivery date.

3.9. CONTRACT TERM

A contract awarded pursuant to this IFB shall have an effective date as provided in the Notice of Award. The term shall be for three (3) years and will expire on the anniversary date of the effective date unless otherwise stated in this Notice of Award, or unless terminated earlier. The State retains the option to extend this contract for one (1) additional one (1) year period.

4.0 FURNISH AND DELIVER

YEAR 1:

ITEM #	QTY	UNIT	DESCRIPTION	UNIT COST	EXTENDED COST
1	1	each	Zilla Security Comply – 1,000 people records		
2	1	each	Connected applications – up to 25		
3	1	each	Onboarding		

Total Offer Cost _____

YEAR 2:

ITEM #	QTY	UNIT	DESCRIPTION	UNIT COST	EXTENDED COST
1	1	each	Zilla Security Comply – 1,000 people records		
2	1	each	Connected applications – up to 25		
3	1	each	Onboarding		

Total Offer Cost _____

YEAR 3:

ITEM #	QTY	UNIT	DESCRIPTION	UNIT COST	EXTENDED COST
1	1	each	Zilla Security Comply – 1,000 people records		
2	1	each	Connected applications – up to 25		
3	1	each	Onboarding		

Total Offer Cost _____

OPTIONAL COSTS: MAY OR MAY NOT BE PURCHASED**OPTION YEAR 1:**

ITEM #	QTY	UNIT	DESCRIPTION	UNIT COST	EXTENDED COST
1	1	each	Zilla Security Comply – 1,000 people records		
2	1	each	Connected applications – up to 25		

Total Offer Cost Years 1-3: _____

Total Offer Cost with Option Year(s): _____

5.0 HISTORICALLY UNDERUTILIZED BUSINESSES

“Historically Underutilized Businesses (HUBs) consist of minority, women and disabled business firms that are at least fifty-one percent owned and operated by an individual(s) of the aforementioned categories. Also included in this category are disabled business enterprises and non-profit work centers for the blind and severely disabled.” <http://ncadmin.nc.gov/businesses/hub>

Pursuant to N.C.G.S. §§143B-1361(a), 143-48 and 143-128.4, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. This includes utilizing subcontractors to perform the required functions in this IFB .

Is Vendor a Historically Underutilized Business? ☐ YES ☐ NO If “YES”, specify classification. _____

6.0 **DEPARTMENT OF INFORMATION TECHNOLOGY INSTRUCTIONS TO VENDORS**

- 1) **READ, REVIEW AND COMPLY:** It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all requirements specified herein.
- 2) **DEFINITIONS:**
 - **NCDIT:** The North Carolina Department of Information Technology, formerly Office of Information Technology Services
 - **NCDIT CONVENIENCE CONTRACT:** A contract that is used for the procurement of IT goods or Services. These contracts are in place for the convenience of the state and use of them is optional.
 - **OPEN MARKET CONTRACT:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
 - **TERM CONTRACT:** A contract in which a source of supply is established for a specified period of time for specified Services or supplies; usually characterized by an estimated or definite minimum quantity, with the possibility of additional requirements beyond the minimum, all at a predetermined unit price
 - **THE STATE:** Is the state of North Carolina and its agencies.
 - **VENDOR:** Company, firm, corporation, partnership, individual, etc., submitting a response to a solicitation.
- 3) **PROMPT PAYMENT DISCOUNTS:** Vendors are urged to compute all discounts into the price offered. If a prompt payment discount is offered, it will not be considered in the award of the contract except as a factor to aid in resolving cases of identical prices.
- 4) **CLARIFICATIONS/INTERPRETATIONS:** Any and all questions regarding this document must be addressed to the purchaser named on the cover sheet of this document. Do not contact the user directly. Any and all revisions to this document shall be made only by written addendum from NCDIT. The Vendor is cautioned that the requirements of this IFB can be altered only by written addendum and that verbal communications from whatever source are of no effect.
- 5) **ACCEPTANCE AND REJECTION:** The State reserves the right to reject any and all offers, to waive any informality in offers and, unless otherwise specified by the Vendor, to accept any item in the offer. If either a unit price or an extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.
- 6) **AWARD OF CONTRACT:** Responsive offers will be evaluated and acceptance may be made in accordance with Best Value procurement practices as defined by N.C.G.S. §143-135.9. Unless otherwise specified by the State or the Vendor, the State reserves the right to accept any item or group of items on a multi-item offer. In addition, on agency specific or term contracts, NCDIT reserves the right to make partial, progressive or multiple awards: where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated requirements as to quantity, quality, delivery, service, geographical areas; other factors deemed by NCDIT to be pertinent or peculiar to the purchase in question.
- 7) **MISCELLANEOUS:** Masculine pronouns shall be read to include feminine pronouns and the singular of any word or phrase shall be read to include the plural and vice versa.
- 8) **PROTEST PROCEDURES:** When an vendor wants to protest a contract awarded pursuant to this solicitation that is over \$25,000 they must submit a written request to the issuing agency at the address given in this document. This request must be received in this office within fifteen (15) calendar days from the date of the contract award, and must contain specific sound reasons and any supporting documentation for the protest. **Note:** Contract award notices are sent **only** to those actually awarded contracts, and not to every person or firm responding to this solicitation. IFB status and Award notices are posted on the Internet at <https://evp.nc.gov>. **All protests will be governed by NCAC Title 9, Department of Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**
- 9) **VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM** The electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and services available on the eVP at the following web site: <https://evp.nc.gov>.

10) DIGITAL IMAGING: The State will digitize the Vendor's response if not received electronically, and any awarded contract together with associated contract documents. This electronic copy shall be a preservation record, and serve as the official record of this solicitation with the same force and effect as the original written documents comprising such record. Any printout or other output readable by sight shown to reflect such record accurately is an "original."

7.0 DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

1) DEFINITIONS:

- a) "Data" includes means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.
- b) Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.
- c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online software applications identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.
- d) "State" shall mean the State of North Carolina, the Department of Information Technology as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.
- e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) ACCESS AND USE OF SAAS SERVICES:

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will

be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

- d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
- h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
- i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.

3) WARRANTY OF NON-INFRINGEMENT; REMEDIES.

- a) Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
- b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become noninfringing. If neither of these options can reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay

those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:

- i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) ACCESS AVAILABILITY; REMEDIES:

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.

If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:

1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10% service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) EXCLUSIONS:

- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;

- ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
- iii) Force Majeure conditions set forth hereinbelow.
- iv) The State's sole misuse of, or its own inability to use, the Services.

6) PERFORMANCE REVIEW AND ACCOUNTABILITY. N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:

- a) Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 et seq., the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

Vendor's Liability for Injury to Persons or Damage to Property:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of this Agreement, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

8) MODIFICATION OF SERVICES: If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.

9) TRANSITION PERIOD:

- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
- b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
- c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
- d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
- e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
- f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.

10) TRANSPORTATION: Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.

11) TRAVEL EXPENSES: All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.

12) PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES: Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements with the Vendor. Violations of this provision may result in debarment of the Vendor(s) or Vendor(s) as permitted by 9 NCAC 06B.1207, or other provision of law.

13) AVAILABILITY OF FUNDS: Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the State for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the State's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement *is expressly contingent upon* the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the State will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to terminate any Services supplied to the State under this Agreement, and relieve the State of any further obligation thereof. The State shall remit payment for Services accepted on or prior to the date of the aforesaid notice in conformance with the payment terms.

14) PAYMENT TERMS:

- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the

Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein, but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.

- b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
- c) For any third party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
- d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
- e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

15) ACCEPTANCE CRITERIA:

- a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.
- b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld, but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

16) CONFIDENTIALITY: The State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1, *et seq.* Such information may include trade secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate information, Products, Services or appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL.**"

By so marking any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions marked "confidential" meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

18) SECURITY OF STATE DATA:

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.
- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:

- i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
- ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
- iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own

expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - (1) The scale and quantity of the State Data loss;
 - (2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and

- (3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
- (4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall investigate of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.
- o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

19) ACCESS TO PERSONS AND RECORDS: Pursuant to N.C. General Statute 147-64.7, the State, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Agreement. Additional audit or reporting requirements may be required by any State, if in the State's opinion, such requirement is imposed by federal or state law or regulation. The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.

20) ASSIGNMENT: Vendor may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days of any consolidation, acquisition, or merger. Any assignee shall affirm this Agreement attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

21) NOTICES: Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand.

22) TITLES AND HEADINGS: Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

23) AMENDMENT: This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.

24) TAXES: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

25) GOVERNING LAWS, JURISDICTION, AND VENUE: This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or

purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and preenforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

26) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the material requirements and specifications herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a. If Vendor fails to deliver or provide correct Services within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide Services or other Deliverables.
- b. Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

27) FORCE MAJEURE: Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

28) COMPLIANCE WITH LAWS: The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.

29) TERMINATION: Any notice or termination made under this Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated. The parties may mutually terminate this Agreement by written agreement at any time.

- a) The State may terminate this Agreement, in whole or in part, pursuant to the Paragraph entitled "Default," above, or pursuant to Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following
 - i) Termination for Cause: In the event any goods, Services, or service furnished by the Vendor during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 7), entitled "Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the

parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.

- ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Services performed in conformance with the Agreement. In the event the Agreement is terminated for the convenience of the State the State will pay for all Services and work performed or delivered in conformance with the Agreement up to the date of termination.

30) DISPUTE RESOLUTION: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

31) SEVERABILITY: In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

32) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT: The Parties agree that the State shall be entitled to any and 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.

33) ELECTRONIC PROCUREMENT: (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract. The E-Procurement fee does not normally apply to services.

- a) Reserved.
- b) Reserved.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Agreement. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

OPTIONAL AI TERMS AND CONDITIONS

The following terms (“**AI Terms**”) are hereby added to and become part of the Agreement as Additional Terms if there is AI in the Vendor response. Capitalized terms not defined in these AI Terms have the meanings given in the Agreement.

1. Definitions:

“AI Features” means large language models (LLMs) or other machine learning (ML) or artificial intelligence (AI) features of the Software or Service. AI Features may include or be in addition to AI Tools.

“AI Tools” means any and all deep learning, machine learning, and other artificial intelligence technologies, including any and all (i) algorithms, heuristics, models, and methodologies, whether in source code, object code, human readable form or other form, (ii) proprietary algorithms, software or other IT Systems that make use of or employ expert systems, natural language processing, computer vision, automated speech recognition, automated planning and scheduling, neural networks, statistical learning algorithms (like linear and logistic regression, support vector machines, random forests, k-means clustering), or reinforcement learning, and (iii) proprietary embodied artificial intelligence and related hardware or equipment.

2) AI Prohibited Absent Authorization. Except as expressly disclosed and described by Vendor and expressly approved in writing by the State, Vendor represents and warrants that it will not provide any Software or other Deliverables, or perform any Services that use or incorporate, in whole or in part, any AI Features or AI Tools (or depends in any way upon any AI Features or AI Tools), including without limitation, any collection or processing of any the State’s Data using any AI Features or AI Tools.

3) AI Warranties. With respect to all AI Features or AI Tools (collectively “AI”) described by the Vendor and approved for use by the State, Vendor warrants that:

- (a) Vendor has accurately identified and fully described all AI for use by the State;
- (b) the AI will (i) perform with a high degree of accuracy in accordance with the Specifications and (ii) not produce materially inaccurate results when used in accordance with the Documentation.
- (c) Vendor will monitor the performance of the AI to ensure continued accuracy in accordance with the Specifications, including processes and policies for the regular assessment and validation of the AI’s outputs.
- (d) Vendor has obtained, and is in compliance with, all rights and licenses necessary to use all AI as described in Vendor’s proposal;
- (e) Vendor has complied with all the Laws and industry standards applicable to (i) Vendor’s development and provision of all AI as described in Vendor’s proposal and (ii) the State’s use of all AI as described in the Vendor’s proposal;
- (f) Vendor specifically represents and warrants that Vendor has complied with all applicable data privacy laws, rules, and regulations, including but not limited to, the training of the AI algorithms and the data used in that training.
- (g) Vendor will comply with all State policies and procedures relating to the use of AI;
- (h) Vendor will notify Customer at least sixty (60) days prior to any material changes pertaining to the AI (in whole or in part);
- (i) Vendor will cooperate and comply with the State’s privacy, security, and proprietary rights questionnaires and assessments concerning all AI and all proposed changes thereto;
- (j) Vendor will, upon the State’s request, allow the State (or its agent) to audit or review all Software, Deliverables, or Services for usage of AI and will provide the State with all related necessary assistance;
- (k) there have been no interruptions in use of Vendor’s AI in the past six (6) months;
- (l) Vendor (i) retains and maintains information in human-readable form that explains or could be used to explain the decisions made or facilitated by the AI, and (ii) maintains such information in a form that can readily be provided to the State upon request;

- (m) Vendor maintains or adheres to industry standard policies and procedures relating to the ethical or responsible use of AI at and by Vendor, including policies, protocols and procedures for
 - (i) developing and implementing AI in a way that promotes transparency, accountability and human interpretability;
 - (ii) identifying and mitigating bias in training data or in the algorithmic model used in AI Tools, including without limitation, implicit racial, gender, or ideological bias; and
 - (iii) management oversight and approval of employees' use or implementation of AI (collectively, "Vendor AI Policies");
 - (n) there has been
 - (i) no actual or alleged non-compliance with any such Vendor AI Policies;
 - (ii) no actual or alleged failure of any AI to satisfy the requirements or guidelines specified in any such Vendor AI Policies;
 - (iii) no claim alleging that any training data used in the development, training, improvement or testing of any AI was falsified, biased, untrustworthy or manipulated in an unethical or unscientific way; and no report, finding or impact assessment by any employee, contractor, or third party that makes any such allegation; and
 - (iv) no request from any Governmental Authority concerning any Vendor AI.
- 4) Use of AI.** The State may submit Data (including in the form of prompts or queries) to the AI ("Inputs") and receive outputs from the AI ("Outputs").
- 5) Training.** Vendor may not use Inputs or Outputs to train or otherwise improve AI Features, except solely for the benefit of the State. Notwithstanding the foregoing, Vendor may use Inputs or Outputs to train or otherwise improve the AI Features, but only if (a) such Inputs and Outputs have been (i) de-identified so that they do not identify the State, its Users or any other person; (ii) aggregated with data across Vendor's other customers; and (b) such use is approved in advance by the State Chief Information Officer or the Using Agency. For these purposes (and without limiting other obligations with respect to the State's Data generally), such Data is provided by the State to the Vendor strictly "AS IS".
- 6) Intellectual Property:**
- (a) Inputs. Except for Vendor's express rights in the Agreement, as between the parties, the State owns Inputs as the State's Data and retains all intellectual property and other rights in the Inputs.
 - (b) Outputs. Outputs are deemed to be State Data, subject to these AI Terms.
- 7) Infringement by Outputs.** With respect to infringement or misappropriation of third-party intellectual property rights by Outputs, should any Outputs become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor at its own expense, shall defend any action brought against the State. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following: i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and, ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- 8) Special Restrictions on Use of AI Features.** The State will not and will not permit anyone else to:
- (a) use the AI Features or any Output to infringe any third-party rights,
 - (b) use the AI Features or any Output to develop, train or improve any AI or ML models (separate from authorized use of the Software or Services under this Agreement),
 - (c) represent any Output as being approved or vetted by Vendor,
 - (d) represent any Output as being an original work or a wholly human-generated work,
 - (e) use the AI Features for automated decision-making that has legal or similarly significant effects on individuals, unless it does so with adequate human review and in compliance with laws applicable to the State, or

(f) use the AI Features for purposes or with effects that are discriminatory, harassing, harmful or unethical.

9) Limitation of Liability Modifications. The Limitation of Vendor's Liability in Section 1 of the NCDIT Terms and Conditions shall not apply to claims for data privacy or intellectual property infringement arising from Vendor's AI.

10) Updates. Vendor's AI has a data cutoff date of [Fill in date]. The State has the right to receive updates to the dataset, notification of those updates, and delivery of those updates made generally available to Vendor's Customers receiving similar AI Services.

11) Confidentiality. Vendor will ensure that the Services and Software, provided via a third-party cloud ("Cloud Service Provider") and AI environment ("Cloud AI Service Environment"), shall maintain strict confidentiality and security of the State's Data. The State's Data will be securely retained within the specific, dedicated Cloud AI Service Environment allocated for the Vendor, and will not contribute to the training of the Vendor's or the Cloud Service Provider's AI models, nor be utilized by any third party outside of the State's express approval (in writing). Upon receipt of a notice from the State, Vendor will remove all State Data from the Cloud AI Service Environment. Vendor will ensure that the governing contractual terms (e.g. terms of service) issued by the Cloud Service Provider include provisions materially consistent with this provision and will identify the forgoing to the State. Vendor will allow Customer to first approve in writing a given Cloud Service Provider and its Cloud AI Service Environment, such approval not to be unreasonably withheld or delayed. If there is any conflict or ambiguity between this provision and the rest of the Agreement, this provision governs and controls so mitigate and correct any security breach.

ATTACHMENT A – AI or GEN AI ASSESSMENT

For Vendor solutions utilizing or incorporating Generative AI (GenAI), please review the State's definitions below and respond **IN YOUR OFFER** to the following series of specifications with details and explanations.

Algorithm: A set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer (NIST Glossary of AI Terms, March 2023).

Artificial Intelligence (AI): Artificial intelligence (AI) is a broad term used to describe an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (International Association of Privacy Professionals, Glossary, <https://iapp.org/resources/glossary/>, 2024). This definition provides a high-level summary of AI definitions found in NIST's *The Language of Trustworthy AI: An In-Depth Glossary of Terms* (March 22, 2023).

Generative AI: A kind of artificial intelligence capable of generating new content such as code, images, music, text (Ex: ChatGPT), simulations, 3D objects, videos, and so on. It is considered an important part of AI research and development, as it has the potential to revolutionize many industries, including entertainment, art, and design (NIST Glossary of AI Terms, March 2023).

Hallucination: Generated content that is nonsensical or unfaithful to the provided source content (NIST Glossary of AI Terms, March 2023).

Machine Learning: The study or the application of computer algorithms that improve automatically through experience. Machine learning algorithms build a model based on training data in order to perform a specific task, like aiding in prediction or decision-making processes, without necessarily being explicitly programmed to do so (NIST Glossary of AI Terms, March 2023).

Personal Information or Identifying Information (PII): As defined in N.C.G.S. 75-61(10) and N.C.G.S. 14-113.22(a), information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

If de-identification of data is performed and Vendor is contractually allowed to use this data for training or other purposes, Vendor may not combine this data with other data sets or perform any other type of data matching to re-identify individuals, and may not use, share, sell, or allow access to the data in a way that allows others to re-identify individuals.

1. Describe the level of intelligence and specific AI technologies the Vendor utilize in their programs. (e.g., machine learning, natural language processing, computer vision).
2. Describe how does the Vendor's proposed AI solution meet the State's definition of AI, GenAI or both.
3. Identify Level of GenAI/AI Autonomy by checking the appropriate box:
 - a. ☐ System operates automatically with no human intervention.
 - b. ☐ System operates automatically with occasional retrospective reviews by humans.
 - c. ☐ System produces recommendations but cannot act without human intervention.
4. Describe the specific use cases and workflows that the Vendor's GenAI/AI system designed to support?
5. Describe the Vendor's AI practices, training, and testing methods.

6. Describe how the Vendor's AI practices, training, and testing methods align with U.S. AI frameworks and guidance for best practices for responsible use of AI, (e.g., NIST AI Risk Management Framework 1.0; The White House Blueprint for an AI Bill of Rights; and [Principles for Responsible Use of AI | NCDIT](#)).
7. Describe the performance indicators and metrics that the Vendor uses to measure effectiveness and efficiency of their AI system.
8. Describe how these performance indicators and metrics are reported and monitored.
9. Does the Vendor use subcontractors?
 - a. If yes, describe how the Vendor ensures that subcontractors adhere to data protection standards, including those required of the Vendor in this RFP.
 - b. Describe Vendor's protocols and protections in place to ensure the subcontractor's compliance with data protection standards and requirements.
10. Describe the type of model(s) and/or network(s) (e.g., generative adversarial networks (GANs), types of neural networks) that will be, or are, used in the GenAI/AI system. Please reference all and explain their specific applicational use and purpose.
11. Describe the measures that Vendor has in place to prevent discriminatory results.
12. Describe the mechanisms that can be used to audit the system and its data.
 - a. Describe who will have access to audit logs.
 - b. Describe the access. Will access be role-based and authenticated?
13. Describe the sources that are used to test and validate the integrity and accuracy of the training model.
14. Describe the Vendor's measures in place to protect data privacy and comply with state and federal law or regulations (e.g., N.C.G.S. Chapter 14, Article 19C, Identity Theft, HIPAA, FERPA).
14. Describe how the Vendor protects State data.
16. Describe how Vendor's protection of State data is operationalized.
17. Describe the method and processes that the Vendor uses to address and eliminate biases in datasets and outputs.
18. Describe how the Vendor will identify and mitigate hallucinations and ensure that GenAI data outputs are accurate and factual.
19. Describe the specific techniques or technologies employed to detect and mitigate hallucinations.
20. Describe and explain Vendor's destruction/sanitization practices (e.g., follows NIST 800-88).
21. Describe the protections that the Vendor uses, or will use, to protect State data, including but not limited to de-identification, anonymization, hashing, or similar processes.
 - a. If de-identification is performed, describe the processes in place to keep data from being re-identified by the Vendor.
 - b. If de-identification is performed, describe how or whether the de-identified data is used, shared, or accessed in any way by the Vendor or others that could allow for reidentification including through matching with other data sets.