

STATE OF NORTH CAROLINA

University of North Carolina at Wilmington (UNCW)

Request for Proposal #: 72-PRAB25027

Website, Email Marketing and Event Management Software solution

Date of Issue: 12/20/2024

Proposal Opening: 1/21/25 virtually via Zoom

at 2:30 PM ET, for submissions uploaded before 2:00 PM EST

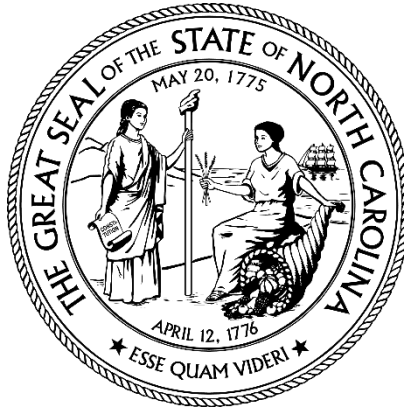
Direct all inquiries concerning this RFP to:

Robert Bisanar

Purchasing Specialist

Email: bisanarr@uncw.edu (PREFERRED)

Phone: 910/962-4069



STATE OF NORTH CAROLINA
University of North Carolina at Wilmington

Request for Proposal

72-PRAB25027

For internal State agency processing, including tabulation of proposals in the electronic Vendor Portal (eVP), please provide your company's Federal Employer Identification Number or alternate identification number (e.g. Social Security Number). Pursuant to G.S. 132-1.10(b) this identification number shall not be released to the public. **This page will be removed and shredded, or otherwise kept confidential**, before the procurement file is made available for public inspection.

**This page is to be filled out and returned with your proposal.
Failure to do so may subject your proposal to rejection.**

ID Number:

Federal ID Number or Social Security Number

Vendor Name

Only electronic responses via eVP will be accepted for this solicitation

STATE OF NORTH CAROLINA
University of North Carolina at Wilmington (UNCW)

Refer <u>ALL</u> Inquiries regarding this RFP to: Contract Lead: Robert Bisanar, CPPB, NCCM Email bisanarr@uncw.edu (PREFERRED) and Phone (910) 962-4069	Request for Proposal # 72-PRAB25027
	Proposals will be publicly opened: 2:30 PM EST, Tuesday, January 21, 2025 with submissions uploaded <u>before</u> 2:00 PM EST
Contract Type: Open Market	Opening Location: Virtual via Zoom
Commodity No. 4323000 – Website, Email Marketing and Event Management software solution	Requisition No.: 193601457

EXECUTION: In compliance with this Request for Proposals (RFP), and subject to all the conditions herein, the undersigned Vendor offers and agrees to furnish and deliver any or all items upon which prices are bid, at the prices set opposite each item within the time specified herein. By executing this proposal, the undersigned Vendor certifies that this proposal is submitted competitively and without collusion (G.S. 143-54), that none of its officers, directors, or owners of an unincorporated business entity has been convicted of any violations of Chapter 78A of the General Statutes, the Securities Act of 1933, or the Securities Exchange Act of 1934 (G.S. 143-59.2), and that it is not an ineligible Vendor as set forth in G.S. 143-59.1. False certification is a Class I felony. Furthermore, by executing this proposal, the undersigned certifies to the best of Vendor's knowledge and belief, that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from covered transactions by any Federal or State department or agency. As required by G.S. 143-48.5, the undersigned Vendor certifies that it, and each of its sub-contractors for any Contract awarded as a result of this RFP, complies with the requirements of Article 2 of Chapter 64 of the NC General Statutes, including the requirement for each employer with more than 25 employees in North Carolina to verify the work authorization of its employees through the federal E-Verify system. G.S. 133-32 and Executive Order 24 (2009) prohibit the offer to, or acceptance by, any State Employee associated with the preparing plans, specifications, estimates for public Contract; or awarding or administering public Contracts; or inspecting or supervising delivery of the public Contract of any gift from anyone with a Contract with the State, or from any person seeking to do business with the State. By execution of this response to the RFP, the undersigned certifies, for your entire organization and its employees or agents, that you are not aware that any such gift has been offered, accepted, or promised by any employees of your organization.

Failure to execute/sign proposal prior to submittal shall render proposal invalid and it WILL BE REJECTED. Late proposals cannot be accepted.

COMPLETE/FORMAL NAME OF VENDOR:		
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY & STATE & ZIP:	TELEPHONE NUMBER:	TOLL FREE TEL. NO:
PRINCIPAL PLACE OF BUSINESS ADDRESS IF DIFFERENT FROM ABOVE (SEE INSTRUCTIONS TO VENDORS ITEM #12):		
PRINT NAME & TITLE OF PERSON SIGNING ON BEHALF OF VENDOR:		FAX NUMBER:
VENDOR'S AUTHORIZED SIGNATURE*	DATE:	EMAIL:
<i>*If submitting an electronic response Vendor has two options: 1) Vendor may apply a wet signature, scan, and then upload this attestation page as an attachment for submission through eVP; or 2) Vendor may apply a digital/electronic signature in the designated box, scan, and then upload as an attachment along with its proposal</i>		

Offer valid for at least 120 days from date of proposal opening, unless otherwise stated here: _____ days.

ACCEPTANCE OF PROPOSAL If any or all parts of this proposal are accepted by the University of North Carolina at Wilmington, an authorized representative of UNCW shall affix his/her signature hereto and this document and all provisions of this Request for Proposal along with the Vendor proposal response and the written results of any negotiations shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the successful Vendor(s).

FOR STATE USE ONLY: Offer accept and Contract awarded this _____ day of _____, 20____, as indicated on the attached certification, by _____ (Authorized Representative of University of North Carolina at Wilmington)

Contents

1.0	PURPOSE AND BACKGROUND	6
2.0	GENERAL INFORMATION.....	6
2.1	REQUEST FOR PROPOSAL DOCUMENT	6
2.2	E-PROCUREMENT SOLICITATION	6
2.3	NOTICE TO VENDORS REGARDING RFP TERMS AND CONDITIONS	6
2.4	RFP SCHEDULE	7
2.5	PROPOSAL QUESTIONS	7
2.6	PROPOSAL SUBMITTAL	7
2.7	PROPOSAL CONTENTS	8
2.8	ALTERNATE PROPOSALS	8
2.9	DEFINITIONS, ACRONYMS, AND ABBREVIATIONS*	8
3.0	METHOD OF AWARD AND PROPOSAL EVALUATION PROCESS.....	9
3.1	METHOD OF AWARD	9
3.2	CONFIDENTIALITY AND PROHIBITED COMMUNICATIONS DURING EVALUATION.....	9
3.3	PROPOSAL EVALUATION PROCESS.....	10
3.4	EVALUATION CRITERIA	11
3.5	PERFORMANCE OUTSIDE THE UNITED STATES	11
3.6	INTERPRETATION OF TERMS AND PHRASES.....	11
4.0	REQUIREMENTS	12
4.1	CONTRACT TERM.....	12
4.2	PRICING.....	12
4.3	INVOICES.....	13
4.4	FINANCIAL STABILITY	13
4.5	REFERENCES	13
4.6	BACKGROUND CHECKS.....	13
4.7	PERSONNEL.....	13
4.8	VENDOR’S REPRESENTATIONS	14
5.0	SCOPE OF WORK, EXPERIENCE, ORGANIZATION, APPROACH, AND QUESTIONS TO VENDORS	14
5.1	GENERAL SCOPE	14
5.2	TASKS/DELIVERABLES	15
5.3	VENDOR EXPERIENCE.....	15
5.4	PROJECT ORGANIZATION.....	16
5.5	TECHNICAL APPROACH	16

5.6	ACCEPTANCE OF WORK	16
5.7	QUESTIONS TO VENDORS	16
5.8	TRANSITION ASSISTANCE	17
6.0	CONTRACT ADMINISTRATION.....	18
6.1	PROJECT MANAGER AND CUSTOMER SERVICE	18
6.2	POST AWARD MANAGEMENT REVIEW MEETINGS	18
6.3	CONTINUOUS IMPROVEMENT.....	18
6.4	DISPUTE RESOLUTION	18
6.5	CONTRACT CHANGES	18
	ATTACHMENT A: PRICING.....	19
	ATTACHMENT B: INSTRUCTIONS TO VENDORS.....	20
	ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS & CONDITIONS	23
	ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR.....	28
	ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION.....	29
	ATTACHMENT F: SUPPLEMENTAL VENDOR INFORMATION	30
	ATTACHMENT G: IT SERVICES & SYSTEMS ADDENDUM	31
	ATTACHMENT H: UNCW E-COMMERCE AND/OR PAYMENT ACCEPTANCE/REMITTANCE SOFTWARE REQUIREMENTS	36

1.0 PURPOSE AND BACKGROUND

The University's Division of University Advancement (UA) is seeking online software, with an existing bi-directional data flow with Blackbaud Raiser's Edge, that can provide website hosting, event management, email marketing and additional robust digital engagement services.

UA is primarily responsible for engaging our institution's alumni and donor populations. Philanthropic campaigns, alumni engagement, academic area promotions and university news are areas of focus. To address increasing software shortcomings and service interruptions, UA is searching for a new technology partner before our contract with Blackbaud NetCommunity (BBNC) ends July 31, 2025. Currently, this product provides limited capabilities in hosting our alumni (alumni.uncw.edu) and giving (giving.uncw.edu) websites, email marketing, event and registration management — and other limited capabilities for enhanced digital engagement solutions, such as bio update forms.

Proposals shall be submitted in accordance with the terms and conditions of this RFP and any addenda issued hereto.

2.0 GENERAL INFORMATION

2.1 REQUEST FOR PROPOSAL DOCUMENT

The RFP is comprised of the base RFP document, any attachments, and any addenda released before Contract award. All attachments and addenda released for this RFP in advance of any Contract award are incorporated herein by reference.

2.2 E-PROCUREMENT SOLICITATION

ATTENTION: This is NOT an E-Procurement solicitation. Section 16 of Attachment C: North Carolina General Contract Terms and Conditions, paragraphs (b) and (c), do not apply to this solicitation.

2.3 NOTICE TO VENDORS REGARDING RFP TERMS AND CONDITIONS

It shall be the Vendor's responsibility to read the Instructions, the State's terms and conditions, all relevant exhibits and attachments, and any other components made a part of this RFP and comply with all requirements and specifications herein. Vendors also are responsible for obtaining and complying with all Addenda and other changes that may be issued in connection with this RFP.

If Vendors have questions, issues, or exceptions regarding any term, condition, or other component within this RFP, those must be submitted as questions in accordance with the instructions in Section 2.5 PROPOSAL QUESTIONS. If the State determines that any changes will be made as a result of the questions asked, then such decisions will be communicated in the form of an RFP addendum. The State may also elect to leave open the possibility for later negotiation and amendment of specific provisions of the Contract that have been addressed during the question and answer period. Other than through this process, the State rejects and will not be required to evaluate or consider any additional or modified terms and conditions submitted with Vendor's proposal, or thereafter. This applies to any language appearing in or attached to the document as part of the Vendor's proposal that purports to vary any terms and conditions or Vendors' instructions herein or to render the proposal non-binding or subject to further negotiation. Vendor's proposal shall constitute a firm offer. **By execution and delivery of this RFP Response, the Vendor agrees that any additional or modified terms and conditions, whether submitted purposely or inadvertently, shall have no force or effect, and will be disregarded. Noncompliance with, or any attempt to alter or delete, this paragraph shall constitute sufficient grounds to reject Vendor's proposal as nonresponsive.**

By executing and submitting its proposal in response to this RFP, Vendor understands and agrees that the State may exercise its discretion not to consider any and all proposed modifications Vendor(s) may request and may accept Vendor's proposal under the terms and conditions of this RFP.

Contact with anyone working for or with the State regarding this RFP other than the State Contract Lead named on the face page of this RFP in the manner specified by this RFP shall constitute grounds for rejection of said Vendor's offer, at the State's election.

2.4 RFP SCHEDULE

The table below shows the *intended* schedule for this RFP. The State will make every effort to adhere to this schedule.

Event	Responsibility	Date and Time
Issue RFP	State	12/20/2024
Submit Written Questions	Vendor	before/by 1/2/25
Provide Response to Questions	State	before/by 1/9/25
Submit Proposals	Vendor	before 2:00 PM EST, 1/21/25
Bid opening	State	2:30 PM EST, 1/21/25
Anticipated Finalists presentations	State and Vendor(s)	Est. 2/17/25 – 2/28/25
Anticipated Contract Award	State	by 3/14/25
Anticipated Contract Effective Date	State	before/by 6/20/25

2.5 PROPOSAL QUESTIONS

Upon review of the RFP documents, Vendors may have questions to clarify or interpret the RFP in order to submit the best proposal possible. To accommodate the Proposal Questions process, Vendors shall submit any such questions by the above due date.

Written questions shall be emailed to the Contract Lead by the date and time specified above. Vendors should enter “RFP # 72-PRAB25011 Questions” as the subject for the email. Questions submittals should include a reference to the applicable RFP section and be submitted in a format shown below:

Reference	Vendor Question
RFP Section, Page Number	Vendor question ...?

Questions received prior to the submission deadline date, the State’s response, and any additional terms deemed necessary by the State will be posted in the form of an addendum to the eVP, and shall become an Addendum to this RFP. 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 RFP, shall be considered authoritative or binding. Vendors shall rely *only* on written material contained in an Addendum to this RFP.

2.6 PROPOSAL SUBMITTAL

IMPORTANT NOTE: This is an absolute requirement. Vendor shall bear the risk for late submission due to unintended or unanticipated delay. It is the Vendor’s sole responsibility to ensure its proposal has been submitted to the online eVP system before 2:00 PM EST. The time and date of submission will be electronically marked on each proposal when received. Any proposal-submitted after the proposal deadline will be rejected.

All proposal responses shall be submitted electronically via the eVP. For additional information, see <https://evp.nc.gov/>.

Failure to submit a proposal in strict accordance with these instructions shall constitute sufficient cause to reject a vendor’s proposal(s).

Critical updated information may be included in Addenda to this RFP. It is important that all Vendors proposing on this RFP periodically check the State’s eVP website for any Addenda that may be issued prior to the bid opening date. All Vendors shall be deemed to have read and understood all information in this RFP and all Addenda thereto.

Contact with anyone working for or with the State regarding this RFP other than the State Contract Lead named on the face page of this RFP in the manner specified by this RFP shall constitute grounds for rejection of said Vendor’s offer, at the State’s election.

2.7 PROPOSAL CONTENTS

Vendors shall populate all attachments of this RFP that require the Vendor to provide information and include an authorized signature where requested. Vendor RFP responses shall include the following items and those attachments should be arranged in the following order:

- a) Cover Letter
- b) Title Page: Include the company name, address, phone number and authorized representative along with the Proposal Number.
- c) Completed and signed version of EXECUTION PAGES, along with the body of the RFP and signed receipt pages of any addenda released in conjunction with this RFP (if required to be returned).
- d) Vendor's Proposal addressing all Specifications of this RFP, not limited to but including:
 - Acknowledgement of Minimum Requirements in Section 4.0,
 - References from Section 4.5
 - The responses to Questions to Vendors in Section 5.4.
- e) Completed version of ATTACHMENT A: PRICING
- f) ATTACHMENT B: INSTRUCTIONS TO VENDORS
- g) ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS AND CONDITIONS
- h) Completed and signed version of ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR
- i) Completed and signed version of ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION
- j) Completed and signed version of ATTACHMENT F: SUPPLEMENTAL VENDOR INFORMATION
- k) ATTACHMENT G: IT SERVICES & SYSTEMS ADDENDUM
- l) ATTACHMENT H: UNCW E-COMMERCE AND/OR PAYMENT ACCEPTANCE/REMITTANCE SOFTWARE REQUIREMENTS

2.8 ALTERNATE PROPOSALS

Vendor may submit alternate proposals for various methods or levels of service(s) or that propose different options. Alternate proposals must specifically identify the RFP requirements and advantage(s) addressed by the alternate proposal. Any alternate proposal, in addition to the marking described above, must be clearly marked with the legend: "Alternate Proposal #___ [for 'name of Vendor']". Each proposal must be for a specific set of Services and must include specific pricing. If a Vendor chooses to respond with various service offerings, each must be offered with a separate price and be contained in a separate proposal document. Each proposal must be complete and independent of other proposals offered.

2.9 DEFINITIONS, ACRONYMS, AND ABBREVIATIONS*

- a) **BAFO:** Best and Final Offer, submitted by a Vendor to alter its initial offer, made in response to a request by the issuing agency.
- b) **BBNC:** Blackbaud NetCommunity
- c) **CONTRACT LEAD / PURCHASING SPECIALIST:** Representative of UNCW identified on the first page of this RFP who will correspond with potential Vendors concerning solicitation issues and will contract with the Vendor providing the best offer to the State, and is the individual who will administer The Contract for the State.
- d) **E-PROCUREMENT SERVICE(S):** Not applicable to this RFP. The fee based program, system, and associated Services through which the State conducts electronic procurement. UNC System schools do not use the State's E-Procurement system.
- e) **eVP:** Electronic Vendor Portal (evp.nc.gov), a free, electronic system for Vendors to view and search for bid opportunities.
- f) **FOB-DESTINATION:** Title changes hand from Vendor to purchaser at the destination point of the shipment; Vendor owns commodity in transit and files any claims, and Vendor pays all freight and any related transportation charges. A solicitation may request Vendors to separately identify freight charges in their proposal, but no amount or charge not

included as part of the total proposal price will be paid.

- g) **MUST:** A term indicating a mandatory requirement.
- h) **ON-TIME DELIVERY:** The delivery of all items within a single order to the receiving point designated by the ordering entity within the delivery time required.
- i) **QUALIFIED PROPOSAL:** A responsive proposal submitted by a responsible Vendor.
- j) **RESPONSIVE PROPOSAL:** A bid proposal that meets all criteria of a bid such as, but not limited to, bid execution, and submittal of all required data within the required timeframe.
- k) **RESPONSIBLE PROPOSER:** Proposer has 1) the skill, judgment, and integrity necessary to faithfully perform the Contract and 2) has sufficient financial resources and 3) has the ability to perform the Contract.
- l) **RE:** Blackbaud Raiser's Edge
- m) **RFP:** Request for Proposal.
- n) **SERVICES or SERVICE DELIVERABLES:** The tasks and duties undertaken by the Vendor to fulfill the requirements and specifications of this solicitation.
- o) **SHALL:** A term indicating a mandatory requirement or action.
- p) **STATE:** The State of North Carolina, including any of its sub-units recognized under North Carolina law.
- q) **THE CONTRACT:** Specifically, a contract between **UNCW** and a successful **VENDOR** which is executed based on an award made pursuant this RFP.
- r) **UA:** The University's Division for University Advancement
- s) **UNIVERSITY:** The University of North Carolina at Wilmington, UNCW, UNC-Wilmington, UNC-W, etc.
- t) **VENDOR:** Contractor, offeror, supplier, bidder, proposer, company, firm, corporation, partnership, individual or other entity submitting a response to a Request for Proposal.

***See additional definitions in ATTACHMENTS G & H.**

3.0 METHOD OF AWARD AND PROPOSAL EVALUATION PROCESS

3.1 METHOD OF AWARD

Contracts will be awarded in accordance with G.S. 143-52 and the evaluation criteria set out in this solicitation. Prospective Vendors shall not be discriminated against on the basis of any prohibited grounds as defined by Federal and State law.

All qualified proposals will be evaluated, and awards will be made to the Vendor(s) meeting the RFP requirements and achieving the highest and best final evaluation, based on the criteria described below.

While the intent of this RFP is to award a Contract(s) to single Vendor, the State reserves the right to make separate awards to different Vendors for one or more line items, to not award one or more line items or to cancel this RFP in its entirety without awarding a Contract, if it is considered to be most advantageous to the State to do so.

The State reserves the right to waive any minor informality or technicality in proposals received.

3.2 CONFIDENTIALITY AND PROHIBITED COMMUNICATIONS DURING EVALUATION

During the evaluation period—from the date proposals are opened through the date the contract is awarded—each Vendor submitting a proposal (including its representatives, sub-contractors and/or suppliers) is prohibited from having any communications with any person inside or outside the using agency, issuing agency, other government agency office, or body (including the purchaser named above, department secretary, agency head, members of the general assembly and/or governor's office), or private entity, if the communication refers to the content of Vendor's proposal or qualifications, the contents of another Vendor's proposal, another Vendor's qualifications or ability to perform the contract, and/or the transmittal of any other communication of information that could be reasonably considered to have the effect of directly or indirectly influencing the evaluation of proposals and/or the award of the contract. A Vendor not

in compliance with this provision shall be disqualified from contract award, unless it is determined in the State's discretion that the communication was harmless, that it was made without intent to influence and that the best interest of the State would not be served by the disqualification. A Vendor's proposal may be disqualified if its sub-contractor and supplier engage in any of the foregoing communications during the time that the procurement is active (i.e., the issuance date of the procurement to the date of contract award). Only those discussions, communications or transmittals of information authorized or initiated by the issuing agency for this RFP or general inquiries directed to the purchaser regarding requirements of the RFP (prior to proposal submission) or the status of the contract award (after submission) are excepted from this provision.

3.3 PROPOSAL EVALUATION PROCESS

The State shall review all Vendor responses to this RFP to confirm that they meet the specifications and requirements of the RFP.

The State will conduct a One-Step evaluation of Proposals:

Proposals will be received from each responsive Vendor according to the method of submission specified in Section 2.6 of this RFP.

All proposals must be received by the issuing agency not later than the date and time specified on the cover sheet of this RFP, or as modified by an RFP addendum.

At that date and time, the proposal from each responding firm will be opened publicly and the name of each Vendor will be announced. Interested parties are cautioned that the proposals are subject to further evaluation for completeness and correctness.

At its option, the State may request clarifications, oral presentations or discussions with any or all Vendors in order to clarify or to amplify the materials presented in any part of the proposal. Vendors are cautioned, however, that the State is not required to request presentations or other clarification—and often does not. Therefore, all proposals should be complete and reflect the most favorable terms available from the Vendor.

Proposals will generally be evaluated according to completeness, content, and experience with similar projects, ability of the Vendor and its staff, and cost. Specific evaluation criteria are listed in 3.4 EVALUATION CRITERIA, below.

Vendors are cautioned that this is a request for offers, not an offer or request to contract, and the State reserves the unqualified right to reject any and all proposals at any time if such rejection is deemed to be in the best interest of the State.

The State reserves the right to reject all original offers and request one or more of the Vendors submitting proposals within a competitive range to submit a best and final offer (BAFO), based on discussions and negotiations with the State, if the initial responses to the RFP have been evaluated and determined to be unsatisfactory.

Upon completion of the evaluation process, the State will make Award(s) based on the evaluation and post the award(s) to eVP under the RFP number for this solicitation. Award of a Contract to one Vendor does not mean that the other proposals lacked merit, but that, all factors considered, the selected proposal was deemed most advantageous and represented the best value to the State.

3.4 EVALUATION CRITERIA

All qualified proposals will be evaluated and award made based on considering the following criteria, to result in an award most advantageous to the State:

Technical (70 Maximum Points)

- Integrations, Training, and Support – 12%
- Website Hosting & Constituent Engagement – 20%
- Email Marketing – 12%
- Event Management – 16%
- Complete acceptance of North Carolina Terms & Conditions, and no additional terms presented – 10%

Price (30 Maximum Points)

Example: The State will determine low cost by normalizing the scores as follows:

The proposal with the lowest cost will receive a score of 30. All other competing proposals will be assigned a portion of the maximum score using the formula:

$$30 \times \frac{\text{the cost of the lowest cost proposal}}{\text{the cost of the cost proposal being evaluated}}$$

3.5 PERFORMANCE OUTSIDE THE UNITED STATES

Vendor shall complete ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR. In addition to any other evaluation criteria identified in this RFP, the State may also consider, for purposes of evaluating proposed or actual contract performance outside of the United States, how that performance may affect the following factors to ensure that any award will be in the best interest of the State:

- a) Total cost to the State
- b) Level of quality provided by the Vendor
- c) Process and performance capability across multiple jurisdictions
- d) Protection of the State's information and intellectual property
- e) Availability of pertinent skills
- f) Ability to understand the State's business requirements and internal operational culture
- g) Particular risk factors such as the security of the State's information technology
- h) Relations with citizens and employees
- i) Contract enforcement jurisdictional issues

3.6 INTERPRETATION OF TERMS AND PHRASES

This Request for Proposal serves two functions: (1) to advise potential Vendors of the parameters of the solution being sought by the Department; and (2) to provide (together with other specified documents) the terms of the Contract resulting from this procurement. As such, all terms in the Request for Proposal shall be enforceable as contract terms in accordance with the General Contract Terms and Conditions. The use of phrases such as "shall," "must," and "requirements" are intended to create enforceable contract conditions. In determining whether proposals should be evaluated or rejected, the Department will take into consideration the degree to which Vendors have proposed or failed to propose solutions that will satisfy the Department's needs as described in the Request for Proposal. Except as specifically stated in the Request for Proposal, no one requirement shall automatically disqualify a Vendor from consideration. However, failure to comply with any single requirement may result in the Department exercising its discretion to reject a proposal in its entirety.

4.0 REQUIREMENTS

This Section lists the requirements and preferences related to this RFP. By submitting a proposal, the Vendor agrees to meet all stated requirements in this Section as well as any other specifications, requirements and terms and conditions stated in this RFP. Vendors should respond to each of the below points. If a Vendor is unclear about a requirement or specification or believes a change to a requirement would allow for the State to receive a better proposal, the Vendor is urged and cautioned to submit these items in the form of a question ONLY during the question and answer period in accordance with Section 2.5.

Vendors should respond after each below, to confirm vendor's ability and/or acceptance of each of the following requirements. Failure to respond to each requirement may result in the vendor's proposal being rejected due to non-responsiveness.

(Minimum) Requirements:

1. The proposed solution has the capabilities to manage UNCW UA areas of need: 1. webpage content, 2. email marketing, 3. events and 4. constituent engagement. **Confirm with Yes or No:** _____
2. Any payment processor must integrate with Fiserv, UNCW's payment processor and the state's only contracted vendor (i.e., settlement must be completed via Fiserv). **Confirm with Yes or No:** _____
3. The proposed solution must integrate to UNCW's accounting/general ledger system (Ellucian Banner). (See additional requirements in ATTACHMENT H: UNCW E-COMMERCE AND/OR PAYMENT ACCEPTANCE/REMITTANCE SOFTWARE REQUIREMENTS) **Confirm ALL requirements met in ATTACHMENT H with Yes or No:** _____
4. The proposed solution provides an automated and bi-directional data flow with Blackbaud Raiser's Edge. **Confirm with Yes or No:** _____
5. The proposed solution's website platform provides an intuitive environment (that does not exclusively require coding) for ease-of use, consistent branding and standardization during webpage creation and webpage and content editing. **Confirm with Yes or No:** _____
6. The proposed solution's website platform has the ability to provide dynamic (variable or customized) content and experiences for end-users who log in. **Confirm with Yes or No:** _____

4.1 CONTRACT TERM

The Contract shall have an initial term of either two (2) or three (3) years, depending on what may be determined as more advantageous to the State, both with options to renew annually for up to an additional three (3) years or two (2) years, respectively (total of possible five years for both), beginning on the date of an installed, implemented, integrated, completed and fully usable, working solution ("Effective Date"). The Vendor shall begin work under the Contract within 14 business days of the Award Date. (See breakout of both options in ATTACHMENT A.)

The State will give the Vendor written notice of its intent whether to exercise each option no later than 30 days before the end of the Contract's then-current term. In addition, the State reserves the right to extend a contract term for a period of up to 180 days in 90-day-or-less increments.

4.2 PRICING

Proposal price shall constitute the total cost to the State for complete performance in accordance with the requirements and specifications herein, including all applicable charges handling, administrative and other similar fees. Vendor shall not invoice for any amounts not specifically allowed for in this RFP. Complete ATTACHMENT A: PRICING FORM and include in Proposal. Additionally, vendors may also provide a breakdown of associated costs for the not to exceed amount provided on this Attachment. However, the form should still be filled out, for ATTACHMENT A.

4.3 INVOICES

- a) Invoices must be submitted to the following address: Accounts Payable, 601 S. College Rd., Wilmington, NC 28403, in lieu of electronically to accountspayable@uncw.edu.
- b) Invoices must bear the correct contract number and purchase order number to ensure prompt payment. The Vendor's failure to include the correct purchase order number may cause delay in payment.
- c) Invoices must include an accurate description of the work for which the invoice is being submitted, the invoice date, the period of time covered, and the amount of fees due to the Vendor.

4.4 FINANCIAL STABILITY

Each Vendor shall certify it is financially stable by completing the ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION. The State is requiring this certification to minimize potential issues from Contracting with a Vendor that is financially unstable. From the date of the Certification to the expiration of the Contract, the Vendor shall notify the State within thirty (30) days of any occurrence or condition that materially alters the truth of any statement made in this Certification.

4.5 REFERENCES

Vendors shall provide *at least* three (3) references for which your company has provided Services of similar size and scope to that proposed herein. The State may contact these users to determine the Services provided are substantially similar in scope to those proposed herein and Vendor's performance has been satisfactory. The information obtained may be considered in the evaluation of the proposal.

INSTITUTION/COMPANY NAME	CONTACT NAME	EMAIL/TELEPHONE NUMBER

4.6 BACKGROUND CHECKS

Any personnel or agent of the Vendor performing Services under any contract arising from this RFP may be required to undergo a background check at the expense of the Vendor, if so requested by the State.

4.7 PERSONNEL

Vendor shall not substitute key personnel assigned to the performance of this Contract without prior written approval by the Contract Lead. Vendor shall notify the Contract Lead of any desired substitution, including the name(s) and references of Vendor's recommended substitute personnel. The State will approve or disapprove the requested substitution in a timely manner. The State may, in its sole discretion, terminate the services of any person providing services under this Contract. Upon such termination, the State may request acceptable substitute personnel or terminate the contract services provided by such personnel.

4.8 VENDOR'S REPRESENTATIONS

- a) Vendor warrants that qualified personnel shall provide Services under this Contract in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the industry. Vendor agrees that it will not enter any agreement with a third party that may abridge any rights of the State under this Contract. Vendor will serve as the prime contractor under this Contract and shall be responsible for the performance and payment of all sub-contractor(s) that may be approved by the State. Names of any third party Vendors or sub-contractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party sub-contractor(s).
- b) If any Services, deliverables, functions, or responsibilities not specifically described in this Contract are required for Vendor's proper performance, provision and delivery of the service and deliverables under this Contract, or are an inherent part of or necessary sub-task included within such service, they will be deemed to be implied by and included within the scope of the contract to the same extent and in the same manner as if specifically described in the contract. Unless otherwise expressly provided herein, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and Deliverables.
- c) Vendor warrants that it has the financial capacity to perform and to continue perform its obligations under the contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of this Contract; and that entering into this Contract is not prohibited by any contract, or order by any court of competent jurisdiction.

5.0 SCOPE OF WORK, EXPERIENCE, ORGANIZATION, APPROACH, AND QUESTIONS TO VENDORS

5.1 GENERAL SCOPE

Due to limitations within the BBNC web/email platform, UA has had to implement a number of workarounds for our BBNC products to remain relevant — and for UA to efficiently and effectively execute UA's needs in hosting UA's websites and utilizing our digital engagement solutions for UA's constituents. UA is seeking a service that can offer digital constituent engagement and content management solutions that align with best practices in higher education, advancement (philanthropic initiatives) and constituent engagement. An online giving platform is not part of this request as UA currently contracts with GiveCampus for online giving and crowdfunding campaigns and does not plan to change this service at this time.

There are six teams within UA's division that will have different responsibilities related to maintaining this solution: communications (this team includes one website administrator and will be the most involved in managing the solution), annual giving, alumni engagement, events, data processing and gift administration. UA closely partners with the university's Information Technology Services for domain setup and renewals along with security compliance, as well as partnering with the office of University Relations for branding guidance to ensure consistency with university platforms.

UA's current database size is approximately 350,000 records. This includes an alumni population of 110,000 as part of a total target audience for outreach of about 180,000 (with donors, students, employees and volunteers). Approximately 300 emails are sent annually with audiences ranging from a few hundred to 110,000 per message.

UA manages, on average, 150 events throughout a calendar year — about three per week. Most events span a few hours while a few, like Homecoming, span a few days and encompass multiple sub-events under the main Homecoming event. Approximately 50% of the events are free to attendees, however, the ability to make a gift (donation) is made available when registering for 90% of the events. There are approximately 160,000 event registrations on an annual basis.

5.2 TASKS/DELIVERABLES

It is preferred that a web, email marketing and event management solution is fully operational by June, 2025, providing the ability to transition away from BBNC before the current contract expires. Access to the solution by April 15, 2025 would be ideal and allow time for staff to begin training and populating content.

- A. The solution shall be mapped to RE for constituent data transfer that includes but not limited to: constituent biographical data such as name, address and email, constituent communication preferences, constituent activities and involvement, event registrations, email analytics and website engagement.

The current solution used by UA allows the ability to define the frequency of data transfer for different activities. For example, email engagement data may feed over to RE every 30 minutes where other data transfers occur daily. Real-time transfers would be expected when external users are viewing their bio data through the websites or when an email is processing to deploy, and the software is retrieving current email addresses from Raiser's Edge. It would be ideal if the proposed solution offered similar options.

- B. The solution shall be mapped to UA's RE database for event data transfer that includes, but is not limited to: event date, ticket types, pricing, capacity and location. This data is intended to integrate with the proposed event registration solution, for ease and efficiency in building registration forms.

- C. Two websites shall be included in the solution, alumni.uncw.edu and giving.uncw.edu, that have the capability to integrate and track analytics within GA4 and Google Tag manager. Currently, giving.uncw.edu has approximately 70 webpages in total and alumni.uncw.edu has approximately 60 webpages in total. Each site has 8-12 templates for which design support is needed for the migration.

1. These websites shall also have the ability for external constituents (alumni, volunteers, etc.) to login and perform actions such as viewing and updating their biographical data, viewing webpages or reference documents applicable to their volunteer activities and involvement, opting in to share their contact information, connecting with fellow alumni through a directory and other enhanced digital engagement that will help UA meet goals.
2. Ideally, the solution would have intuitive and robust capabilities for managing website content that limits the need for front-end development while providing dynamic and interactive capabilities for content, such as news modules.

- D. Upwards of 20 UA staff members shall have administrator access to the solution, which would include four (4) high-level administrators that require full access and the remaining to have varied view or edit permissions for email marketing, website content and event registration management.

- E. The solution's email marketing capabilities shall provide the ability to personalize messages through dynamic/conditional content and merge fields, pulling from data in RE.

UA prefers the ability to see all engagement for each recipient, including but not limited to: time opened, device and inbox type, and attributed transactions (event registrations, bio form completions, for example). Within the proposed solution, the ability to identify engaged segments that would benefit from follow-up outreach would be ideal. This would allow UA to build out automation strategies or outreach campaigns that are more sophisticated than a single touch point.

5.3 VENDOR EXPERIENCE

In its Proposal, Vendor shall demonstrate experience with public and/or private sector clients with similar or greater size and complexity to the State of North Carolina. Vendor shall provide information as to the qualifications and experience of all executive, managerial, legal, and professional personnel to be assigned to this project, including resumes citing experience with similar projects and the responsibilities to be assigned to each person.

5.4 PROJECT ORGANIZATION

Vendor shall describe the organizational and operational structure it proposes to utilize for the work described in this RFP, and identify the responsibilities to be assigned to each person Vendor proposes to staff the work.

5.5 TECHNICAL APPROACH

Vendor's proposal shall include, in narrative, outline, and/or graph form the Vendor's approach to implementing and maintaining the proposed solution throughout the entire contract term. An onboarding and training timeline should be provided that identifies how the university will be able to implement the new websites, email marketing and event management solution by June 20, 2025. The timeline should include when the university would be granted access to tools and begin training with the awarded solution, which is preferred to be by April 15, 2025.

5.6 ACCEPTANCE OF WORK

In the event acceptance criteria for any work or deliverables is not described in contract documents or work orders hereunder, the State shall have the obligation to notify Vendor, in writing thirty (30) calendar days following completion of such work or deliverable described in the Contract that it is not acceptable. The notice shall specify in reasonable detail the reason(s) it is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for reasonable review, evaluation, installation or testing, as applicable of the work or deliverable. Final acceptance is expressly conditioned upon completion of all applicable assessment procedures. Should the work or deliverables fail to meet any requirements, acceptance criteria or otherwise fail to conform to the contract, the State may exercise any and all rights hereunder, including, for deliverables, such rights provided by the Uniform Commercial Code as adopted in North Carolina.

5.7 QUESTIONS TO VENDORS

Vendor shall respond to each of the following (15) questions. Vendors are requested to keep responses straightforward and to the point and should not include generic marketing material, however it's encouraged to be as descriptive as a vendor is able. Responses will be reviewed as part of the evaluation process.

General	
1.	In addition to Blackbaud Raiser's Edge, share with what other constituent databases the proposed solution integrates.
2.	Describe what client specific, non-prerecorded/in-person (virtual) training is available during onboarding and throughout the contract period. If additional costs are associated with training (not included with the proposed services), please explain.
3.	Describe what support is available to new clients after the launch and onboarding period, as part of the agreement. Explain any additional expenses that could be incurred after the onboarding process concludes.
Website Hosting & Constituent Engagement	
4.	Describe the proposed solution's ability to host multiple subdomains and the support provided for setting these up and maintaining them during the contract period (i.e. annual SSL certificate renewal and DNS verification). Please share associated costs, if any.
5.	Explain the dynamic (variable or customized) content and experiences that can be made available for end-users who log in.
6.	Describe the proposed solution's form/survey capabilities and what (if anything) may be available for end users who are logged in. In this response, include an end user's ability to upload images.

- | |
|--|
| 7. Describe the website platform's news module capabilities. (For example: comprehensive news listing formats, landing page news scrolls, tickers, etc.) |
| 8. Describe in detail the proposed solution's integrations with Google Analytics/GA4 and what other analytics tools that may exist within the software, and whether clients have the ability to manage triggers and tracking for specific pages and content areas, or if the analytics integrations are only managed sitewide. |

Email Marketing

- | |
|--|
| 9. Describe the email marketing environment and the expected workflow for clients using the software. This should also describe the solution's intuitiveness for easy-to-use email building that doesn't require coding. Explain whether templates or modules can be created for drag-and-drop updating that maintains consistency and brand standards. Also describe how audience lists are connected to emails and opt-outs tracked. |
| 10. Explain the proposed solution's capabilities for merging variable data (either from RE or an imported data list) and creating dynamic content for audience segments. |
| 11. Describe the analytics provided and what (if any) data is shared with RE. |

Event Management

- | |
|--|
| 12. Describe the capabilities of the event management solution. (i.e. multi-day events, different ticket types such as paid and unpaid, discount codes, ability for end-users to accept or decline, manages walk-up registrations, ability to duplicate for future events, etc.) |
| 13. Describe how the event registration data syncs with the RE events module and the record of a registered constituent. |
| 14. Describe how the event management registration form provides the ability to include a donation (to a fund in RE) as part of the registration process. |
| 15. Describe the types of communications the proposed solution provides that are associated with event registrations (confirmations, reminders, etc.) for both registrants and our organization (if any). |

5.8 TRANSITION ASSISTANCE

If this Contract is not renewed at the end of the term, or is canceled prior to its expiration, for any reason, Vendor shall provide, at the option of the State, up to six (6) months after such end date all such reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. If the State exercises this option, the Parties agree that such transition assistance shall be deemed to be governed by the terms and conditions of this Contract (notwithstanding this expiration or cancellation), except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Contract for performance of the Services or other resources utilized.

6.0 CONTRACT ADMINISTRATION

6.1 PROJECT MANAGER AND CUSTOMER SERVICE

The Vendor shall designate and make available to the State a project manager. The project manager shall be the State's point of contact for contract related issues and issues concerning performance, progress review, scheduling and service.

6.2 POST AWARD MANAGEMENT REVIEW MEETINGS

The Vendor, at the request of the State, shall meet periodically [e.g., weekly, monthly] with the State for Project Review meetings, as requested by the requesting UNCW department. The purpose of these meetings will be to review project progress reports, discuss Vendor and State performance, address outstanding issues, review problem resolution, provide direction, evaluate continuous improvement and cost saving ideas, and discuss any other pertinent topics.

6.3 CONTINUOUS IMPROVEMENT

The State encourages the Vendor to identify opportunities to reduce the total cost the State. A continuous improvement effort consisting of various ideas to enhance business efficiencies will be discussed at the periodic Business Review Meetings.

6.4 DISPUTE RESOLUTION

The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the State's Contract Lead for resolution. A claim by the State shall be submitted in writing to the Vendor's Project Manager for resolution. 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 Contract. 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 Contract, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

6.5 CONTRACT CHANGES

Contract changes, if any, over the life of the contract shall be implemented by contract amendments agreed to in writing by the State and Vendor.

THIS SECTION IS INTENTIONALLY LEFT BLANK.

ATTACHMENT A: PRICING

For this attachment, Vendors should still provide pricing below, however may additionally provide a separate attachment/documentation, by noting "SEE ATTACHED", here:

Pricing option # 1 (two year agreement with three options to renew, annually):

Vendors should provide a total not to exceed, first year's (annual) cost for the provided solution/service here: \$ _____

Vendors should provide costs for the second year here: \$ _____

Vendors should provide costs for an optional (third year) extension here: \$ _____

Vendors should provide costs for an optional (fourth year) extension here: \$ _____

Vendors should provide costs for an optional (fifth year) extension here: \$ _____

Pricing option # 2 (three year agreement, with two options to renew, annually):

Vendors should provide a total not to exceed, first year's (annual) cost for the provided solution/service here: \$ _____

Vendors should provide costs for the second year here: \$ _____

Vendors should provide costs for the third year here: \$ _____

Vendors should provide costs for an optional (fourth year) extension here: \$ _____

Vendors should provide costs for an optional (fifth year) extension here: \$ _____

Again, in addition to providing annual costs on ATTACHMENT A, here, vendors may also attach a separate document, specifically to break out the associated costs that may occur, if not lump sum annual costs, particularly for the first year. Vendors should describe the pricing model and what is encompassed in the proposed prices above.

This may include, although would not be limited to milestones, if not invoiced in full, upon the completion of the proposed solution's use, as described in Section 4.1 CONTRACT TERM, working up to the Effective Date. Vendors may also provide relevant information in this attachment section, including but not limited to associated costs for additional options, which are outside of the scope of this RFP.

ATTACHMENT B: 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 any addenda thereto, and comply with all requirements specified herein, regardless of whether appearing in these Instructions to Vendors or elsewhere in this RFP document.
2. **LATE PROPOSALS:** Late proposals, regardless of cause, will not be opened or considered, and will automatically be disqualified from further consideration. It shall be the Vendor's sole responsibility to ensure the timely submission of proposals at the designated office by the designated time.
3. **ACCEPTANCE AND REJECTION:** The State reserves the right to reject any and all proposals, to waive any informality in proposals and, unless otherwise specified by the Vendor, to accept any item in the proposal.
4. **BASIS FOR REJECTION:** Pursuant to 01 NCAC 05B .0501, 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 requirements 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 any 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.
5. **EXECUTION:** Failure to execute page 3 of the RFP (Execution Page) in the designated space shall render the proposal non-responsive, and it will be rejected.
6. **ORDER OF PRECEDENCE:** In cases of conflict between specific provisions in this solicitation or those in any resulting contract documents, the order of precedence shall be (high to low) (1) any special terms and conditions specific to this RFP, including any negotiated terms; (2) requirements and specifications and administration provisions in Sections 4, 5 and 6 of this RFP; (3) North Carolina General Contract Terms and Conditions in ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS AND CONDITIONS and ATTACHMENT G: IT SERVICES & SYSTEMS ADDENDUM; (4) Instructions in ATTACHMENT B: INSTRUCTIONS TO VENDORS; (5) ATTACHMENT A: PRICING, and (6) Vendor's proposal.
7. **INFORMATION AND DESCRIPTIVE LITERATURE:** Vendor shall furnish all information requested in the spaces provided in this document. Further, if required elsewhere in this proposal, each Vendor shall submit with its proposal any sketches, descriptive literature and/or complete specifications covering the products and Services offered. Reference to literature submitted with a previous proposal or available elsewhere will not satisfy this provision. Failure to comply with these requirements shall constitute sufficient cause to reject a proposal without further consideration.
8. **RECYCLING AND SOURCE REDUCTION:** It is the policy of the State to encourage and promote the purchase of products with recycled content to the extent economically practicable, and to purchase items which are reusable, refillable, repairable, more durable and less toxic to the extent that the purchase or use is practicable and cost-effective. We also encourage and promote using minimal packaging and the use of recycled/recyclable products in the packaging of commodities purchased. However, no sacrifice in quality of packaging will be acceptable. The Vendor remains responsible for providing packaging that will adequately protect the commodity and contain it for its intended use. Vendors are strongly urged to bring to the attention of purchasers those products or packaging they offer which have recycled content and that are recyclable.
9. **CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA:** As a condition of contract award, each out-of-State Vendor that is a corporation, limited-liability company or limited-liability partnership shall have received, and shall maintain throughout the term of The Contract, a Certificate of Authority to Transact Business in North Carolina from the North Carolina Secretary of State, as required by North Carolina law. A State contract requiring only an isolated transaction completed within a period of six months, and not in the course of a number of repeated transactions of like nature, shall not be considered as transacting business in North Carolina and shall not require a Certificate of Authority to Transact Business.
10. **SUSTAINABILITY:** To support the sustainability efforts of the State of North Carolina we solicit your cooperation in this effort. Pursuant to Executive Order 156 (1999), it is desirable that all print responses submitted meet the following:
 - All copies of the proposal are printed double sided.
 - All submittals and copies are printed on recycled paper with a minimum post-consumer content of 30%.

- Unless absolutely necessary, all proposals and copies should minimize or eliminate use of non-recyclable or non-reusable materials such as plastic report covers, plastic dividers, vinyl sleeves, and GBC binding. Three-ringed binders, glued materials, paper clips, and staples are acceptable.
- Materials should be submitted in a format which allows for easy removal, filing and/or recycling of paper and binder materials. Use of oversized paper is strongly discouraged unless necessary for clarity or legibility.

11. **HISTORICALLY UNDERUTILIZED BUSINESSES:** The State is committed to retaining Vendors from diverse backgrounds, and it invites and encourages participation in the procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. In particular, the State encourages participation by Vendors certified by the State Office of Historically Underutilized Businesses, as well as the use of HUB-certified vendors as sub-contractors on State contracts.
12. **RECIPROCAL PREFERENCE:** G.S. 143-59 establishes a reciprocal preference requirement to discourage other states from favoring their own resident Vendors by applying a percentage increase to the price of any proposal from a North Carolina resident Vendor. To the extent another state does so, North Carolina applies the same percentage increase to the proposal of a vendor resident in that state. Residency is determined by a Vendor's "Principal Place of Business," defined as that principal place from which the overall trade or business of the Vendor is directed or managed.
13. **INELIGIBLE VENDORS:** As provided in G.S. 147-86.60 and G.S. 147-86.82, the following companies are ineligible to contract with the State of North Carolina or any political subdivision of the State: a) any company identified as engaging in investment activities in Iran, as determined by appearing on the Final Divestment List created by the State Treasurer pursuant to G.S. 147-86.58, and b) any company identified as engaged in a boycott of Israel as determined by appearing on the List of restricted companies created by the State Treasurer pursuant to G.S. 147-86.81. A contract with the State or any of its political subdivisions by any company identified in a) or b) above shall be void *ab initio*.
14. **CONFIDENTIAL INFORMATION:** To the extent permitted by applicable statutes and rules, the State will maintain as confidential trade secrets in its proposal that the Vendor does not wish disclosed. As a condition to confidential treatment, each page containing trade secret information shall be identified in boldface at the top and bottom as "CONFIDENTIAL" by the Vendor, with specific trade secret information enclosed in boxes, marked in a distinctive color or by similar indication. Cost information shall not be deemed confidential under any circumstances. Regardless of what a Vendor may label as a trade secret, the determination whether it is or is not entitled to protection will be determined in accordance with G.S. 132-1.2. Any material labeled as confidential constitutes a representation by the Vendor that it has made a reasonable effort in good faith to determine that such material is, in fact, a trade secret under G.S. 132-1.2. Vendors are urged and cautioned to limit the marking of information as a trade secret or as confidential so far as is possible. If a legal action is brought to require the disclosure of any material so marked as confidential, the State will notify Vendor of such action and allow Vendor to defend the confidential status of its information.
15. **PROTEST PROCEDURES:** When a Vendor wishes to protest the award of contract awarded by UNCW valued in an awarded amount of at least \$25,000, but less than \$500,000, the Vendor shall submit a written request addressed to the Director of Purchasing Services within thirty (30) consecutive calendar days from the date of the Contract award. The Director of Purchasing Services shall furnish a copy of this letter to the Vice Chancellor for Business Affairs (VCBA) within 5 consecutive calendar days of receipt. The Vendor's letter shall contain specific grounds and reasons for the protest, how the protesting party was harmed by the award made and any documentation providing support for the protesting party's claims. If the protest meeting is granted, the Director of Purchasing Services shall attempt to schedule the meeting within fifteen (15) consecutive calendar days after receipt of the letter, or as soon as possible thereafter. Within 5 consecutive calendar days from the date of the protest meeting, the Director of Purchasing Services shall respond to the Vendor in writing with his decision. A copy of the letter shall be forwarded to the Vice Chancellor for Business Affairs. The University shall notify the State Purchasing Officer, in writing, of any further administrative or judicial review of the contract award. **Note:** Contract award notices are sent only to the Vendor actually awarded the Contract, and not to every person or firm responding to a solicitation. Proposal status and Award notices are posted on the Internet at <https://evp.nc.gov>. All protests will be handled pursuant to the North Carolina Administrative Code, 01 NCAC 05B .1519.
16. **MISCELLANEOUS:** Any gender-specific pronouns used herein, whether masculine or feminine, shall be read and construed as gender neutral, and the singular of any word or phrase shall be read to include the plural and vice versa.
17. **COMMUNICATIONS BY VENDORS:** In submitting its proposal, the Vendor agrees not to discuss or otherwise

reveal the contents of its proposal to any source, government or private, outside of the using or issuing agency until after the award of the Contract or cancellation of this RFP. All Vendors are forbidden from having any communications with the using or issuing agency, or any other representative of the State concerning the solicitation, during the evaluation of the proposals (i.e., after the public opening of the proposals and before the award of the Contract), unless the State directly contacts the Vendor(s) for purposes of seeking clarification or another reason permitted by the solicitation. A Vendor shall not: (a) transmit to the issuing and/or using agency any information commenting on the ability or qualifications of any other Vendor to provide the advertised good, equipment, commodity; (b) identify defects, errors and/or omissions in any other Vendor's proposal and/or prices at any time during the procurement process; and/or (c) engage in or attempt any other communication or conduct that could influence the evaluation or award of a Contract related to this RFP. Failure to comply with this requirement shall constitute sufficient justification to disqualify a Vendor from a Contract award. Only those communications with the using agency or issuing agency authorized by this RFP are permitted.

18. **TABULATIONS:** Bid tabulations can be electronically retrieved at the eVP, <https://evp.nc.gov>. Lengthy or complex tabulations may be summarized, with other details not made available on eVP, and requests for additional details or information concerning such tabulations cannot be honored.
19. **VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM:** The North Carolina electronic Vendor Portal (eVP) allows Vendors to electronically register for free with the State to receive electronic notification of current procurement opportunities for goods and Services of potential interests to them available on the Interactive Purchasing System, as well as notifications of status changes to those solicitations. Online registration and other purchasing information is available at the following website: <https://www.doa.nc.gov/divisions/purchase-contract>.
20. **WITHDRAWAL OF PROPOSAL:** Proposals submitted electronically may be withdrawn at any time prior to the date for opening proposals identified on the cover page of this RFP (or such later date included in an Addendum to the RFP). Proposals that have been delivered by hand, U.S. Postal Service, courier or other delivery service may be withdrawn **only** in writing and if receipt is acknowledged by the office issuing the RFP prior to the time for opening proposals identified on the cover page of this RFP (or such later date included in an Addendum to the RFP). Written withdrawal requests shall be submitted on the Vendor's letterhead and signed by an official of the Vendor authorized to make such request. Any withdrawal request made after the opening of proposals shall be allowed only for good cause shown and in the sole discretion of the State.
21. **INFORMAL COMMENTS:** The State shall not be bound by informal explanations, instructions or information given at any time by anyone on behalf of the State during the competitive process or after award. The State is bound only by information provided in writing in this RFP and in formal Addenda issued through eVP.
22. **COST FOR PROPOSAL PREPARATION:** Any costs incurred by Vendor in preparing or submitting offers are the Vendor's sole responsibility; the State of North Carolina will not reimburse any Vendor for any costs incurred or associated with the preparation of proposals.
23. **VENDOR'S REPRESENTATIVE:** Each Vendor shall submit with its proposal the name, address, and telephone number of the person(s) with authority to bind the firm and answer questions or provide clarification concerning the firm's proposal.
24. **INSPECTION AT VENDOR'S SITE:** If and as applicable, the State reserves the right to inspect, at a reasonable time, the equipment, item, plant or other facilities of a prospective Vendor prior to Contract award, and during the Contract term as necessary for the State's determination that such equipment, item, plant or other facilities conform with the specifications/requirements and are adequate and suitable for the proper and effective performance of the Contract.

ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS & CONDITIONS

- 1) **PERFORMANCE AND DEFAULT:** It is anticipated that the tasks and duties undertaken by the Vendor shall include services or the manufacturing, furnishing, or development of goods and other tangible features or components as deliverables that are directly correlated and/or ancillary to the services performed. Except as provided immediately below, and unless otherwise mutually agreed in writing prior to award, any service deliverables or ancillary services provided by Vendor in performance of the contract shall remain property of the State. During performance, Vendor may provide proprietary components as part of the service deliverables that are identified in the solicitation response. Vendor grants the State a personal, permanent, non-transferable license to use such proprietary components of the service deliverables and other functionalities, as provided under this Agreement. Any 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 agrees to perform its services under the contract in the same or similar manner provided to comparable users. The State shall notify the Vendor of any defects or deficiencies in performance of its services or failure of service deliverables to conform to the standards and specifications provided in this solicitation. Vendor agrees to remedy defective performance or any nonconforming deliverables upon timely notice provided by the State.

Vendor has a limited, non-exclusive license to access and use State Data provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as may be further provided herein. Vendor or its suppliers shall at a minimum, and except as otherwise specified and agreed herein, provide assistance to the State related to all services performed or deliverables procured hereunder during the State's normal business hours. Vendor warrants that its support, customer service, and assistance will be performed in accordance with generally accepted and applicable industry standards.

If, through any cause, Vendor shall fail to fulfill in a timely and proper manner the obligations under The Contract, the State shall have the right to terminate The Contract by giving written notice to the Vendor and specifying the effective date thereof. In that event, any or all finished or unfinished deliverables under The Contract prepared by the Vendor shall, at the option of the State, become its property, and the Vendor shall be entitled to receive just and equitable compensation for any acceptable work completed as to which the option is exercised. Notwithstanding, Vendor shall not be relieved of liability to the State for damages sustained by the State by virtue of any breach of The Contract, and the State may withhold any payment due the Vendor for the purpose of setoff until such time as the exact amount of damages due the State from such breach can be determined. The State may require at any time a performance bond or other acceptable alternative performance guarantees from a Vendor without expense to the State.

In the event of default by the Vendor, the State may procure the goods and services necessary to complete performance hereunder from other sources and hold the Vendor responsible for any excess cost occasioned thereby. In addition, in the event of default by the Vendor under The Contract, or upon the Vendor filing a petition for bankruptcy or the entering of a judgment of bankruptcy by or against the Vendor, the State may immediately cease doing business with the Vendor, immediately terminate The Contract for cause, and may take action to debar the Vendor from doing future business with the State.

- 2) **GOVERNMENTAL RESTRICTIONS:** In the event any Governmental restrictions are imposed which necessitate alteration of the goods, material, quality, workmanship or performance of the Services offered prior to acceptance, it shall be the responsibility of the Vendor to notify the Contract Lead at once, in writing, indicating the specific regulation which required such alterations. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Contract.
- 3) **AVAILABILITY OF FUNDS:** Any and all payments to the Vendor shall be dependent upon and subject to the availability of funds to the agency for the purpose set forth in The Contract.
- 4) **TAXES:** Any applicable taxes shall be invoiced as a separate item.
- a) G.S. 143-59.1 bars the Secretary of Administration from entering into Contracts with Vendors if the Vendor or its affiliates meet one of the conditions of G.S. 105-164.8(b) and refuses to collect use tax on sales of tangible personal property to purchasers in North Carolina. Conditions under G.S. 105-164.8(b) include: (1) Maintenance of a retail establishment or office, (2) Presence of representatives in the State that solicit sales or transact business on behalf of the Vendor and (3) Systematic exploitation of the market by media-assisted, media-facilitated, or media-solicited means. By execution of the proposal document the Vendor certifies that it and all of its affiliates, (if it has affiliates), collect(s) the appropriate taxes.
 - b) The agency(ies) participating in The Contract are exempt from Federal Taxes, such as excise and

transportation. Exemption forms submitted by the Vendor will be executed and returned by the using agency.

- c) Prices offered are not to include any personal property taxes, nor any sales or use tax (or fees) unless required by the North Carolina Department of Revenue.

5. **SITUS AND GOVERNING LAWS:** This Contract is made under and shall be governed and construed in accordance with the laws of the State of North Carolina, without regard to its conflict of laws rules, and within which State all matters, whether sounding in Contract or tort or otherwise, relating to its validity, construction, interpretation and enforcement shall be determined.

6. **PAYMENT TERMS:** Payment terms are Net not later than 30 days after receipt of a correct invoice or acceptance of goods, whichever is later. The using agency is responsible for all payments to the Vendor under the Contract. Payment by some agencies may be made by procurement card, if the Vendor accepts that card (Visa, MasterCard, etc.) from other customers, and it shall be accepted by the Vendor for payment under the same terms and conditions as any other method of payment accepted by the Vendor. If payment is made by procurement card, then payment may be processed immediately by the Vendor.

7. **NON-DISCRIMINATION:**

The Vendor will take necessary action to comply with all Federal and State requirements concerning fair employment and employment of people with disabilities and concerning the treatment of all employees without regard to discrimination on the basis of any prohibited grounds as defined by Federal and State law.

The vendor will take necessary action to ensure its internal employee policies and procedures are consistent with Executive Order #82 (December 6, 2018), which extends workplace protections and accommodations to pregnant employees.

8. **CONDITION AND PACKAGING:** Unless otherwise provided by special terms and conditions or specifications, it is understood and agreed that any item offered or shipped has not been sold or used for any purpose and shall be in first class condition. All containers/packaging shall be suitable for handling, storage or shipment.

9. **INTELLECTUAL PROPERTY WARRANTY AND INDEMNITY:** Vendor shall hold and save the State, its officers, agents and employees, harmless from liability of any kind, including costs and expenses, resulting from infringement of the rights of any third party in any copyrighted material, patented or patent-pending invention, article, device or appliance delivered in connection with The Contract.

- a. Vendor warrants to the best of its knowledge that:
 - i. Performance under The Contract does not infringe upon 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 deliverables 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 deliverables, or replace or modify the same to become non-infringing. 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 deliverables and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute deliverables. If, in the sole opinion of the State, the cessation of use by the State of any such deliverables 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 or Deliverables.
- 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 deliverables 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 deliverables or services, or from the continued use of the deliverable(s) or Services after receiving notice of infringement on a trade secret of a third party.

10. **TERMINATION FOR CONVENIENCE:** If this contract contemplates deliveries or performance over a period of time, the State may terminate this contract at any time by providing sixty [60] days' notice in writing from the State to the Vendor. In that event, any or all finished or unfinished deliverables prepared by the Vendor under this contract shall, at the option of the State, become its property. If the contract is terminated by the State as provided in this section, the State shall pay for those items for which such option is exercised, less any payment or compensation previously made.
11. **ADVERTISING:** Vendor agrees not to use the existence of The Contract or the name of the State of North Carolina as part of any commercial advertising or marketing of products or Services. A Vendor may inquire whether the State is willing to act as a reference by providing factual information directly to other prospective customers.
12. **ACCESS TO PERSONS AND RECORDS:** During and after the term hereof, the State Auditor and any using agency's internal auditors shall have access to persons and records related to The Contract to verify accounts and data affecting fees or performance under the Contract, as provided in G.S. 143-49(9).
13. **ASSIGNMENT:** No assignment of the Vendor's obligations nor the Vendor's right to receive payment hereunder shall be permitted.

However, upon written request approved by the issuing purchasing authority and solely as a convenience to the Vendor, the State may:

- a) Forward the Vendor's payment check directly to any person or entity designated by the Vendor, and
- b) Include any person or entity designated by Vendor as a joint payee on the Vendor's payment check.

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 Contract obligations. Upon advance written request, the State may, in its unfettered discretion, approve an assignment to the surviving entity of a merger, acquisition or corporate reorganization, if made as part of the transfer of all or substantially all of the Vendor's assets. Any purported assignment made in violation of this provision shall be void and a material breach of The Contract.

14. **INSURANCE:**

COVERAGE - During the term of the Contract, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Contract. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

- a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of \$500,000.00, covering all of Vendor's employees who are engaged in any work under the Contract in North Carolina. If any work is sub-contracted, the Vendor shall require the sub-contractor to provide the same coverage for any of his employees engaged in any work under the Contract within the State.
- b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$1,000,000.00 Combined Single Limit. Defense cost shall be in excess of the limit of liability.
- c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used within North Carolina in connection with the Contract. The minimum combined single limit shall be \$250,000.00 bodily injury and property damage; \$250,000.00 uninsured/under insured motorist; and \$2,500.00 medical payment.

REQUIREMENTS - Providing and maintaining adequate insurance coverage is a material obligation of the Vendor and is of the essence of The Contract. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or The Contract. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Contract.

- 15. GENERAL INDEMNITY:** The Vendor shall hold and save the State, its officers, agents, and employees, harmless from liability of any kind, including all claims and losses accruing or resulting to any other person, firm, or corporation furnishing or supplying work, Services, materials, or supplies in connection with the performance of The Contract, and from any and all claims and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Vendor in the performance of The Contract and that are attributable to the negligence or intentionally tortious acts of the Vendor provided that the Vendor is notified in writing within 30 days from the date that the State has knowledge of such claims. The Vendor represents and warrants that it shall make no claim of any kind or nature against the State's agents who are involved in the delivery or processing of Vendor deliverables or Services to the State. The representation and warranty in the preceding sentence shall survive the termination or expiration of The Contract.
- 16. ELECTRONIC PROCUREMENT [RESERVED]:** This is NOT an E-Procurement solicitation
- 17. SUBCONTRACTING:** Performance under The Contract by the Vendor shall not be subcontracted without prior written approval of the State's assigned Contract Lead. Unless otherwise agreed in writing, acceptance of a Vendor's proposal shall include approval to use the sub-contractor(s) that have been specified therein.
- 18. CONFIDENTIALITY:** Any State information, data, instruments, documents, studies or reports given to or prepared or assembled by or provided to the Vendor under The Contract shall be kept as confidential, used only for the purpose(s) required to perform The Contract and not divulged or made available to any individual or organization without the prior written approval of the State.
- 19. CARE OF STATE DATA AND PROPERTY:** The Vendor agrees that it shall be responsible for the proper custody and care of any data owned and furnished to the Vendor by the State (State Data), or other State property in the hands of the Vendor, for use in connection with the performance of The Contract or purchased by or for the State for The Contract. Vendor will reimburse the State for loss or damage of such property while in Vendor's custody.
- The State's Data in the hands of the Vendor shall be protected from unauthorized disclosure, loss, damage, destruction by a natural event or other eventuality. Such State Data shall be returned to the State in a form acceptable to the State upon the termination or expiration of this Agreement. The Vendor shall notify the State of any security breaches within 24 hours as required by G.S. 143B-1379. See G.S. 75-60 *et seq.*
- 20. OUTSOURCING:** Any Vendor or sub-contractor providing call or contact center services to the State of North Carolina or any of its agencies shall disclose to inbound callers the location from which the call or contact center services are being provided.
- If, after award of a contract, the contractor wishes to relocate or outsource any portion of performance to a location outside the United States, or to contract with a sub-contractor for any such performance, which sub-contractor and nature of the work has not previously been disclosed to the State in writing, prior written approval must be obtained from the State agency responsible for the contract.
- Vendor shall give notice to the using agency of any relocation of the Vendor, employees of the Vendor, sub-contractors of the Vendor, or other persons providing performance under a State contract to a location outside of the United States.
- 21. COMPLIANCE WITH LAWS:** Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and its performance in accordance with The Contract, including those of federal, state, and local agencies having jurisdiction and/or authority.
- 22. ENTIRE AGREEMENT:** This RFP and any documents incorporated specifically by reference represent the entire agreement between the parties and supersede all prior oral or written statements or agreements. This RFP, any addenda hereto, and the Vendor's proposal are incorporated herein by reference as though set forth verbatim.
- All promises, requirements, terms, conditions, provisions, representations, guarantees, and warranties contained herein shall survive the contract expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable Federal or State statutes of limitation.
- 23. ELECTRONIC RECORDS:** The State will digitize all Vendor responses to this solicitation, if not received electronically, as well as any awarded contract together with associated procurement-related documents. These electronic copies shall constitute a preservation record and shall serve as the official record of this procurement with the same force and effect as the original written documents comprising such record. Any electronic copy, printout or other output readable by sight shown to reflect such record accurately shall constitute an "original."
- 24. AMENDMENTS:** This Contract may be amended only by a written amendment duly executed by the State and the

Vendor.

- 25. NO WAIVER:** Notwithstanding any other language or provision in The Contract, nothing herein is intended nor shall be interpreted as a waiver of any right or remedy otherwise available to the State under applicable law. The waiver by the State of any right or remedy on any one occasion or instance shall not constitute or be interpreted as a waiver of that or any other right or remedy on any other occasion or instance.
- 26. FORCE MAJEURE:** 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.
- 27. SOVEREIGN IMMUNITY:** Notwithstanding any other term or provision in The Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity or other State or federal constitutional provision or principle that otherwise would be available to the State under applicable law.
- 28. PERSONAL IDENTIFYING INFORMATION:** If the University provides the Vendor with personal identifiers as listed in N.C.G.S. §132-1.10 and in N.C.G.S. §14-133.20(b) or any other legally confidential information including “personally identifiable information” from student education records as defined by the Family Educational Rights and Privacy Act (FERPA), 34 CFR §99.3, Vendor hereby certifies that collection of this information from University is necessary for the performance of Vendor’s duties and responsibilities on behalf of the University under this Contract. Vendor further certifies that it shall maintain the confidential and exempt status of any social security number information, as required by N.C.G.S. §132-1.10(c)(1), and that it shall not re-disclose personally identifiable information as directed by FERPA, 34 CFR §99.33, or other State and Federal laws. Failure to abide by legally applicable security measures and disclosure restrictions may result in the interruption, suspension and/or termination of the relationship with Vendor for a period of at least five (5) years from date of violation. If Vendor experiences a security breach, as defined in N.C.G.S. §75.61(14), relating to this information, in addition to the Vendor’s responsibilities under the NC Identity Theft Protection Act, Vendor shall immediately notify the University with a minimum of information required under N.C.G.S. 75-65 and shall fully cooperate with the University.
- 29. USE OF PRIMARY AGREEMENT BY THIRD PARTIES:** It is the intent of this Agreement to allow for cooperative procurement strictly to those entities within the University of North Carolina. Accordingly, within the University of North Carolina, any constituent institution may access the Sub-Agreement. Participation in this cooperative procurement is strictly voluntary. If authorized by vendor, and agreed to in writing by the University, this Agreement may extend to the entities indicated above to purchase at fees in accordance with the Agreement. Vendor will notify the University in writing of any such entities accessing the Agreement. No modification of this Agreement or execution of a separate agreement is required by a third party in order to participate. If requested by University, vendor will provide semi-annual usage reports for all entities accessing this Sub-Agreement. Participating entities will be bound by the MA and this Agreement; will place their own orders directly with vendor, and will fully and independently administer their use of the Agreement to include contractual disputes, invoicing and payments without direct administration from the University. The University will not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by vendor to extend the Agreement. It is understood and agreed that the University is not responsible for the acts or omissions of any entity, and will not be considered in default of the Agreement. Use of this Agreement does not preclude any participating entity from signing other agreements or competitive processes as the need may be.
- 30. PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS) COMPLIANCE:** In the event Vendor may have access to credit or debit card information and/or may affect the security of a credit or debit card transaction, Vendor agrees to comply with the Payment Card Industry Data Security Standards for itself and any of its sub-contractors.

ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with NC General Statute 143-59.4, the Vendor shall detail the location(s) at which performance will occur, as well as the manner in which it intends to utilize resources or workers outside of the United States in the performance of this Contract. The State will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award. Please complete items a, b, and c below.

a) **Will any work under this Contract be performed outside the United States?** ☐ YES ☐ NO

If the Vendor answered "YES" above, Vendor must complete items 1 and 2 below:

1. List the location(s) outside the United States where work under this Contract will be performed by the Vendor, any sub-contractors, employees, or other persons performing work under the Contract:

2. Describe the corporate structure and location of corporate employees and activities of the Vendor, its affiliates or any other sub-contractors that will perform work outside the U.S.:

b) **The Vendor agrees to provide notice, in writing to the State, of the relocation of the Vendor, employees of the Vendor, sub-contractors of the Vendor, or other persons performing services under the Contract outside of the United States** ☐ YES ☐ NO

NOTE: All Vendor or sub-contractor personnel providing call or contact center services to the State of North Carolina under the Contract **shall** disclose to inbound callers the location from which the call or contact center services are being provided.

c) **Identify all U.S. locations at which performance will occur:**

ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION

Name of Vendor: _____

The undersigned hereby certifies that: [check all applicable boxes]

- ☐ The Vendor is in sound financial condition and, if applicable, has received an unqualified audit opinion for the latest audit of its financial statements.

Date of latest audit: _____

- ☐ The Vendor has no outstanding liabilities, including tax and judgment liens, to the Internal Revenue Service or any other government entity.
- ☐ The Vendor is current in all amounts due for payments of federal and state taxes and required employment-related contributions and withholdings.
- ☐ The Vendor is not the subject of any current litigation or findings of noncompliance under federal or state law.
- ☐ The Vendor has not been the subject of any past or current litigation, findings in any past litigation, or findings of noncompliance under federal or state law that may impact in any way its ability to fulfill the requirements of this Contract.
- ☐ He or she is authorized to make the foregoing statements on behalf of the Vendor.

Note: This is a continuing certification and Vendor shall notify the Contract Lead within fifteen (15) days of any material change to any of the representations made herein.

If any one or more of the foregoing boxes is NOT checked, Vendor shall explain the reason in the space below:

Signature _____ Date _____

Printed Name _____ Title _____

[This Certification must be signed by an individual authorized to speak for the Vendor]

ATTACHMENT F: SUPPLEMENTAL VENDOR INFORMATION

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 categories. Also included in this category are disabled business enterprises and non-profit work centers for the blind and severely disabled.

Pursuant to 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 sub-contractors to perform the required functions in this RFP. Any questions concerning NC HUB certification, contact the [North Carolina Office of Historically Underutilized Businesses](#) at (919) 807-2330. The Vendor shall respond to question #1 and #2 below.

- a) Is Vendor a Historically Underutilized Business? ☐ **Yes** ☐ **No**
- b) Is Vendor Certified with North Carolina as a Historically Underutilized Business? ☐ **Yes** ☐ **No**

If so, state HUB classification: _____

ATTACHMENT G: IT SERVICES & SYSTEMS ADDENDUM

Vendor acknowledges that UNCW will disclose Personally Identifying Information (PII) to the Vendor during the performance of this Agreement, and/or the Agreement allows the Vendor access to PII. Vendor agrees to maintain strict confidentiality of PII, in accordance with the requirements and conditions set forth in this Addendum.

Vendor attests and warrants that any documentation submitted or supplied is accurate, complete, and is a comprehensive assessment of the requirements for which it is submitted. Vendor shall immediately notify the University of any errors, omissions, corrections, or material changes in the documentation and/or underlying information used to prepare the documentation. The University assumes no responsibility to verify the documentation.

1) DEFINITIONS:

- a) "Data" is information, formulae, algorithms, or other content that UNCW, UNCW's employees, agents and end users provide, 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 UNCW's Data may be ascertainable. All data provided or derived is the property of UNCW and is to be confidential and kept private unless otherwise noted by mutual agreement.
- b) "Regulated data" means Personally Identifiable Information (PII) and any other Data that is protected or regulated by state or federal law.
- c) "Services" are the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this Agreement.
- d) "Support" includes provision of ongoing service updates, fixes, training, consulting, and maintenance for Vendor supplied services.
- e) "Personally Identifiable Information", or "PII", is any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data. Personally Identifiable Information shall include "Education Records" and "Personnel Information" as those terms are further defined herein.

2) ACCESS AND USE OF IT SERVICES:

- a) Vendor grants UNCW a personal non-transferable and non-exclusive right to use and access, all contracted Services. UNCW may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. UNCW is authorized to access UNCW Data and any data provided as part of the contracted Services. Services may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. UNCW shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. All Services and information designated as "confidential" or "proprietary", and all Data, 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) UNCW's right to license 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, unless otherwise agreed to by the parties. Vendor has a limited, non-exclusive license to access and use UNCW Data as provided to Vendor, but solely for providing the specified contracted Services.
- c) The technical and professional activities required for establishing, managing, and maintaining the Services and environment are the responsibility of the Vendor.
- d) Any additional agreements or terms derived by end user assent (e.g., "clickthrough") are null and void.
- e) All UNCW Data must remain within the legal jurisdiction of the United States unless the Data's disposition is otherwise explicitly designated by UNCW.
- f) The Vendor is ultimately responsible for providing the contracted Services under the specified provisions. The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, but Vendor assumes all responsibility for third party activities in those regards. Vendor will not provide Data to any subcontractor or agent without UNCW's prior written consent, and until the subcontractor or agent agrees in writing to comply with these Terms and Conditions.

3) MODIFICATION OF SERVICES:

If Vendor modifies or replaces the Services provided to UNCW and other tenants, and if UNCW has paid all applicable Subscription Fees, as that term may be defined in Vendor documentation, UNCW 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 UNCW 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 UNCW until the newer version is provided to UNCW and accepted. If a modification materially affects the functionality of the Services as used by UNCW, at its sole option, UNCW may defer such modification.

4) TRANSITION PERIOD:

- a) For a minimum of ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist UNCW, upon written request, in extracting and/or transitioning all Data in the format determined by UNCW ("Transition Period").
- b) The Transition Period and terms may be modified as specified by both parties in writing.
- c) During the Transition Period, Services access shall continue to be made available to UNCW without alteration.
- d) Vendor agrees to compensate UNCW for damages or losses UNCW incurs as a result of Vendor's failure to comply with this Transition Period section.
- e) Upon termination, and unless otherwise stated in an SLA, and after providing UNCW Data to UNCW as indicated above in this section with acknowledged receipt by UNCW in writing, the Vendor shall permanently destroy or render inaccessible all UNCW Data. The vendor shall provide written documentation confirming the destruction or inaccessibility of UNCW's Data.

5) CONFIDENTIALITY:

UNCW may maintain the confidentiality of certain types of information provided by Vendor 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, or 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.** UNCW 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 UNCW to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending UNCW, including any public official(s) or public employee(s). The Vendor agrees that it shall hold UNCW and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against UNCW in the action. UNCW shall have the right, at its option and expense, to participate in the defense of the action through its counsel. UNCW 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.

6) SECURITY OF UNCW DATA:

- a) All materials, including software, Data, information, and documentation provided by UNCW to the Vendor (UNCW Data) during the performance or provision of Services hereunder are the property of UNCW and must be kept secure, returned to UNCW, and afterwards destroyed. The Vendor will protect UNCW Data from disclosure, unauthorized modification, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to UNCW 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 UNCW as part of the Services.
- b) The Vendor shall protect the confidentiality and integrity of all information, Data, instruments, studies, reports, records and other materials provided to it by UNCW or maintained or created in accordance with provided services. No such information, Data, instruments, studies, reports, records, other materials, or derivatives of such, in the possession of Vendor, shall be disclosed in any form without the prior written consent from UNCW Purchasing.
- c) The Vendor is responsible for the protection of UNCW Data, including but not limited to Personal Identifying Information (PII). Vendor acknowledges its responsibility for securing any UNCW Data used in connection with the provision of the Services. Vendor warrants, it shall provide reasonable care and efforts to protect private and Regulated Data, detect

fraudulent activity involving such Data, and promptly notify UNCW Purchasing of any unauthorized access, use, or Data loss. Specific terms and conditions for Personally Identifiable Information are included herein.

- d) Vendor will provide and maintain secure backups of UNCW Data on an acceptable periodic schedule.
- e) Vendor shall implement and maintain appropriate access controls 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 the Data and the Services from loss, corruption, unauthorized disclosure.
- f) Vendor will apply the principle of "least privilege" for employee and contractor access in providing the contracted services.
- g) Vendor must maintain logs of all changes in user privilege and any access to data.
- h) Upon request Vendor must provide UNCW with the most recent report, audit, or certification, performed by a third party, that relates to the security, availability, processing integrity, confidentiality, and privacy of the operations and systems of the Vendor.
- i) UNCW may, at any time, make a local copy of all UNCW data.
- j) Vendor shall certify to UNCW:
 - i. They have and adhere to a periodically tested and annually reviewed disaster recovery plan.
 - ii. That the Services will comply with the following where applicable:
 - 1. Privacy provisions of the Federal Privacy Act of 1974;
 - 2. The Family Educational Rights and Privacy Act (FERPA) if records include student information.
 - 3. The Health Insurance Portability and Accountability Act if records include any health-based information.
 - 4. The Americans with Disabilities Act and Section 504 of the Rehabilitation Act requirements for access to and use of their provided services.
 - 5. 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);
 - 6. The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - 7. Applicable 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 Computing Guidelines.
- k) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60) means (1) any circumstance pursuant to which 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 UNCW Data or UNCW 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 UNCW Data or UNCW confidential information described in Section 1 above, whether or not by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording,

organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying. Notwithstanding the above, Vendor shall, within one business day of discovery, report to UNCW any use or disclosure of PII not authorized by these Terms and Conditions or in writing by UNCW. Vendor's report shall identify:

- (1) the nature of the unauthorized use or disclosure;
- (2) the PII used or disclosed;
- (3) who made the unauthorized use or received the unauthorized disclosure;
- (4) what Vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
- (5) what corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure.

UNCW, in its sole discretion, shall have the right to require Vendor to submit to a plan of monitoring and reporting; provide Vendor with a fifteen (15) day period to cure the breach; or terminate the Agreement immediately if cure is not possible, subject to Vendor's obligations upon termination described in this paragraph 6. Vendor shall provide any such other information relevant to UNCW's breach investigation and mitigation, including a written report, as reasonably requested by UNCW.

l) 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 UNCW Purchasing of such Security Breach and perform a root cause analysis thereon,
- (2) investigate such Security Breach,
- (3) provide a remediation plan, acceptable to UNCW, 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 UNCW, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach.

UNCW shall make the final decision on notifying UNCW's persons, entities, employees, service providers and/or the general 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 UNCW's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by UNCW) shall be considered legally required. If the Family Policy Compliance Office of the U.S. Department of Education determines that the Vendor improperly disclosed PII obtained from UNCW's Education Records, UNCW may not allow the Vendor access to Education Records for at least five (5) years.

m) Notification Related Costs. Vendor shall reimburse UNCW for all Notification Related Costs incurred by UNCW 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 UNCW'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 UNCW 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 UNCW'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 UNCW's opinion, under the circumstances. In the event that 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 UNCW Purchasing 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.

n) In the event of disaster or catastrophic failure that results in significant UNCW Data loss or extended loss of access to Data or Services, Vendor shall notify UNCW Purchasing by the fastest means available and also in writing, with additional notification provided to the UNCW Chief Information Officer or designee. 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 UNCW of:

- i. The scale and quantity of UNCW Data loss;
- ii. What Vendor has done or will do to recover the UNCW Data from backups and mitigate any deleterious effect of UNCW Data and Services loss; and
- iii. What corrective action Vendor has taken or will take to prevent future UNCW Data and Services loss.
- iv. If Vendor fails to respond immediately and remedy the failure, UNCW may exercise its options for assessing damages or other remedies.

Vendor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with UNCW. UNCW 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 UNCW, its agents and law enforcement.

o) 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 UNCW Data or any other UNCW confidential information or refuse for any reason, to promptly return to UNCW Data and any other UNCW confidential information (including copies thereof) if requested to do so on such media as reasonably requested by UNCW, even if UNCW is then or is alleged to be in breach of the Agreement as long as UNCW has paid any undisputed sums. As a part of Vendor's obligation to provide UNCW Data pursuant to this Paragraph 10)o), Vendor will also provide UNCW any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for UNCW to use, translate, interpret, extract and convert UNCW Data.

7) CONFIDENTIALITY OF EDUCATION RECORDS AND PERSONNEL INFORMATION

a) Education Records

- i. **Definition: Education Records** shall have the meaning prescribed to it in 34 CFR § 99.3, and includes paper and electronic student education record information supplied by UNCW, as well as any data provided by UNCW's students to the Vendor, excluding any information that is designated as "directory information" in UNCW Policy 04.150 Student Records and Family Educational Rights and Privacy Act (FERPA).
- ii. **Protection of Education Records:** Vendor agrees to abide by the limitations on re-disclosure of personally identifiable information from education records set forth in the Family Educational Rights and Privacy Act (34 CFR § 99.33(a)(2)) and with the terms set forth below. 34 CFR § 99.33 (a)(2) states that the officers, employees and agents of a party that receives education record information from the institution may use the information, but only for the purposes for which the disclosure was made.
- iii. **School Official Designation:** For purposes of this Agreement and receipt of Education Records, Vendor is a school official with a legitimate educational interest as defined in 34 CFR § 99.31(a)(1)(i)(B).

b) Personnel Information

- i. **Definition: Personnel Information** shall mean staff and faculty identification numbers beginning with "850," and, to the extent applicable, confidential information contained in an employee's personnel file as provided in N.C.G.S. §§ 126-22 *et seq.*
- ii. **Vendor Designation:** To the extent N.C.G.S. § 132-6 applies, Vendor acknowledges that it is not a custodian of public records under that statute.

c) Ownership and Use of Education and Personnel Records

- i. **Property of UNCW:** Education Records and Personnel Information shall remain the sole property of UNCW. Vendor expressly acknowledges and agrees that Vendor has no property right or interest whatsoever in any such data.
- ii. **Prohibition on Unauthorized Use or Disclosure of Education Records:** Vendor agrees to hold Education Records and Personnel Information in strict confidence. Vendor shall not use or disclose Education Records and Personnel Information received from or on behalf of UNCW except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by UNCW. Vendor agrees not to use Education Records and Personnel Information for any purpose other than the purpose for which the disclosure was made. In the event that Vendor receives a request for Education Records and Personnel Information by subpoena or other legal process or from a court, governmental authority, accrediting agency, or other third party, Vendor shall give prompt written notice to UNCW.

8) PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS) COMPLIANCE:

In the event Vendor may have access to credit or debit card information and/or may affect the security of a credit or debit card transaction, Vendor is required to maintain PCI compliance. Vendor will provide documentation of PCI compliance per the PCI Security Standards Council (www.pcisecuritystandards.org) for itself and any of its third-party vendors, contractors, and service providers used for services provided to the university. Vendor will provide annually a PCI Security Standards Council Attestation of Compliance (AOC), preferably signed by a registered QSA firm, to the university.

ATTACHMENT H: UNCW E-COMMERCE AND/OR PAYMENT ACCEPTANCE/REMITTANCE SOFTWARE REQUIREMENTS

The following are requirements for any UNCW E-Commerce and/or Payment Acceptance/Remittance software (COTS = commercial off the shelf software, whether a Software-as-a-Service [a.k.a., SaaS] or on premises solution) or other vendor solution:

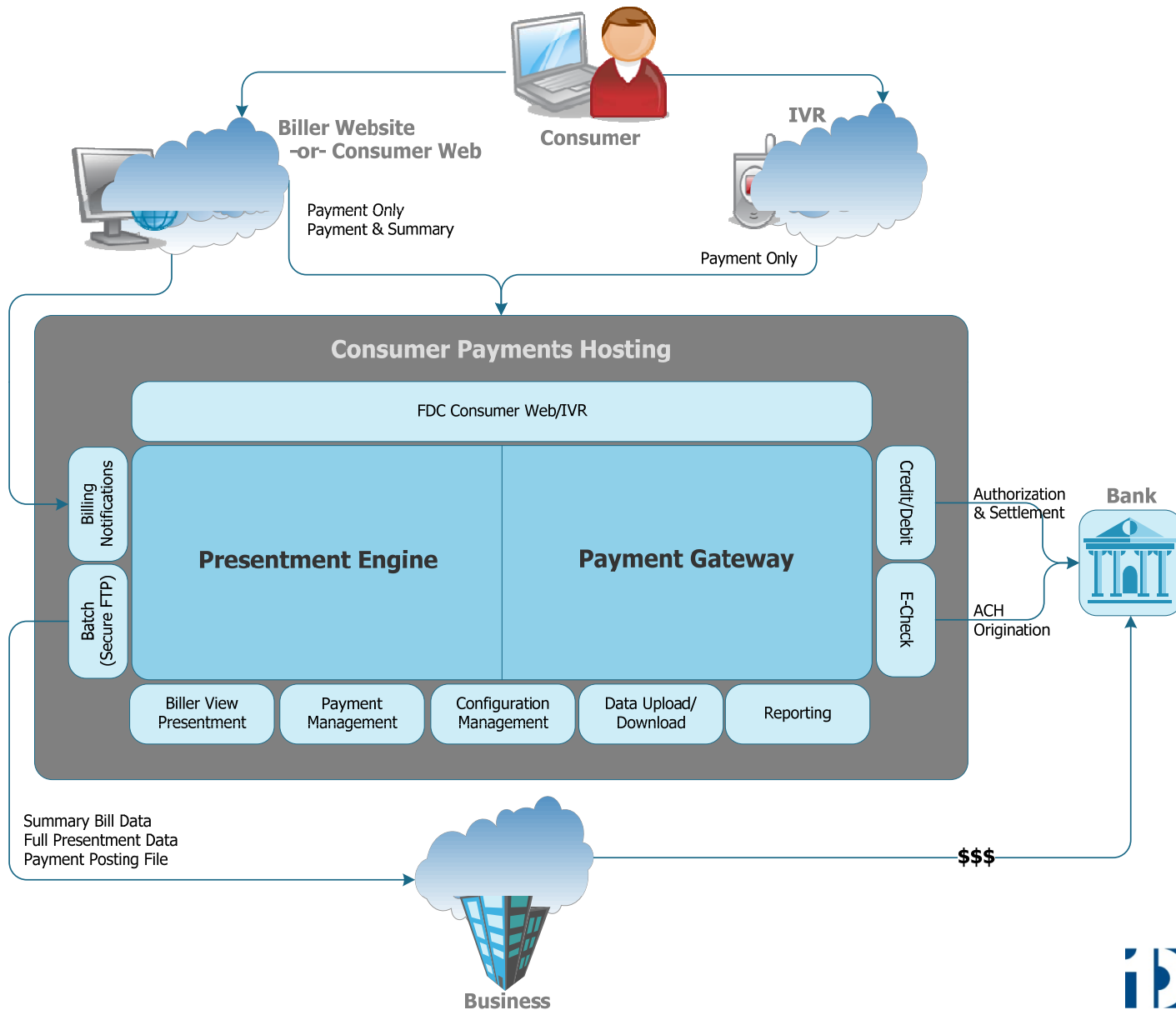
1. Any payment processor must integrate with Fiserv, UNCW's payment processor and the state's only contracted vendor. (I.e., Settlement must be completed via Fiserv.)
2. Must integrate to UNCW's accounting / general ledger system (Ellucian Banner).
3. For any technology stack that is used for a solution, UNCW must be allowed to run a quarterly security vulnerability scan using the State of North Carolina's contracted vendor service or an agreed upon similar scan subject to approval by the UNCW E-Commerce team that can be used for audit and compliance purposes required by UNCW and the State of North Carolina Office of State Controller (OSC).
4. Vendor may select a secure gateway service of its choosing, provided it acquires approval from UNCW (via the OSC exception process) that I have discussed) and adheres to all applicable procurement requirements of the State of North Carolina, UNC System Office, and UNCW.
5. Provide an architectural diagram depicted similar to the attached file showing a First Data Business-to-Consumer (UNCW is B2C for most, B2B for some) architecture. Vendors should have their own architecture diagram and provide their product road map for the upcoming 3-year period to the UNCW E-commerce team and UNCW ITS team to review, evaluate, and discuss. The road map should include release, maintenance, fix, and other planned updates/upgrades for all functionality and features, and include any change in technologies (including versions/releases and why the change is occurring).
6. Provide an annual attested report associated with the vendors SAQ and HECVAT in a secure manner to UNCW each April while the vendor is under contract to UNCW. (The vendor(s) may provide their current annual SAQ as long as it has been attested to and filed with the appropriate organizations.)
7. Provide any financial information requested by UNCW on the company/organization's that states the fiscal health of the organization (such as an annual report and most recent 2 quarterly financial reports regardless of whether a publicly traded or privately held organization).
8. Provide any notification of any breach or suspected breach of the vendor's system and organization within 30-calendar days of the breach occurrence or suspected occurrence once detected. This is a requirement for each breach and/or suspected breach of the vendor's organization network, systems, application, and data. This includes reports of card data and card holder data that was potentially involved in any breach or suspected breach. (UNCW's ITS Security and UNCW's E-Commerce team are to be on the notification list.)
9. Provide assistance for any suspected fraud and / or identity theft related to any card data and card holder data that the vendor solution may have processed in any way (whether failed, hold, refund, purchase, or error) required by the FTC Red Flags rule.
10. Provide support to the UNCW E-Commerce team for vendor services stated in any agreed upon Service Level Agreements (or other written agreements) and the UNCW UA department for all contracted solutions and services. UNCW's E-Commerce team must be named on the authorized call list / access list to speak with the vendor in the event support is required that involves fraud and/or identity theft, any integration with Fiserv, and any other e-commerce support services for the vendor solution. This requirement applies to all Service Level Agreements that are agreed upon by UNCW and the vendor, including any vendors that are part of the solution stack in any way.

UNCW's preference is for the use of TouchNet as a payment platform (TouchNet is currently owned by Heartland, a payment processor that integrates with Fiserv).

This set of requirements allows flexibility to provide UNCW departments the ability to seek a solution that conforms and complies with all UNCW, UNC System Office, Office of State Controller, and Federal applicable rules, regulations, requirements, standards, and guidelines. These requirements conform and comply with all UNCW policies and procedures, audits (including security vulnerability scans), and e-commerce and payment acceptance / remittance practices at UNCW. All solutions must be approved the UNCW Payment Acceptance Committee prior to final purchase execution and implementation of any vendor solution(s) per UNCW policy. An exception process that is listed in requirement #4 above must be initiated by the contracting UNCW Department in conjunction and partnership with the UNCW Payment Acceptance Committee via the UNCW E-Commerce team.

See also attached Consumer Payments Architecture and Small Merchant Glossary of Payment and Information Security Terms.

Consumer Payments Architecture



Glossary of Payment and Information Security Terms



Introduction

This *Glossary of Payment and Information Security Terms* is a supplement to the [Guide to Safe Payments](#), part of the Data Security Essentials for Small Merchants. Its intent is to explain relevant Payment Card Industry (PCI) and information security terms in easy-to-understand language.

Definitions for terms marked with an asterisk (*) are based on or derived from definitions in the [Payment Card Industry \(PCI\) Data Security Standard \(DSS\) and Payment Application Data Security Standard \(PA-DSS\): Glossary of Terms, Abbreviations, and Acronyms](#). The latest version of this glossary is considered the authoritative source, and must be referred to for the current and complete PCI DSS and PA-DSS definitions.

Please refer to the Data Security Essentials for Small Merchants at the following:

RESOURCE	URL
<i>Guide to Safe Payments</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
<i>Common Payment Systems</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
<i>Questions to Ask Your Vendors</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
<i>Evaluation Tool</i>	https://www.pcisecuritystandards.org/merchants/ This tool is provided for merchant information only. An option for merchants is to use it as a first step to gain insight about security practices relevant to the way they accept payments, to provide their initial responses, and to see their results.

Glossary

TERM	DEFINITION
Acquirer *	See <i>Merchant Bank</i> and <i>Payment Processor</i> .
Anti-Virus Software *	Software program that detects, removes, and protects against malicious software (also called “malware”) including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits. Also called “anti-malware software.”
Application *	Software program or group of programs that runs on a PC, smartphone, tablet, internal server, or web server.
Approved Scanning Vendor (ASV) *	Company approved by the PCI Security Standards Council to conduct external vulnerability scanning services to identify common weaknesses in system configuration.
Authentication *	Method for verifying the identity of a person, device, or process attempting to access a computer. To confirm the identity/user is valid, one or more of the following is provided: <ul style="list-style-type: none"> • A password or passphrase (something the user knows) • A token, smart card, or digital certificate unique to the user (something the user has) • A biometric identifier, such as a fingerprint (something the user is or does)
Authorization *	In a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Bank Identification Number (BIN)	The first six digits (or more) of a payment card number that identifies the financial institution that issued the payment card to the cardholder.
Business Need-to-Know	The principle that access to systems or data is granted by a user’s business need—only what is necessary for a user’s job function.
Card Data / Customer Card Data *	At a minimum, card data includes the primary account number (PAN), and may also include cardholder name and expiration date. The PAN is visible on the front of the card and encoded into the card’s magnetic stripe and/or the embedded chip. Also referred to as cardholder data. See also <i>Sensitive Authentication Data</i> for additional data elements which may be part of a payment transaction but which must not be stored after the transaction is authorized.
Chip	Also known as “EMV Chip.” The microprocessor (or “chip”) on a payment card used when processing transactions in accordance with the international specifications for EMV transactions.
Chip and PIN	A verification process where a consumer enters their PIN in an EMV Chip-enabled payment terminal when they purchase goods or services.

Glossary

TERM	DEFINITION
Chip and Signature	A verification process where a consumer uses their signature with an EMV Chip-enabled payment terminal when they purchase goods or services.
Credential	Information used to identify and authenticate a user for access to a system. For example, credentials are often the username and password. Credentials may include a fingerprint, retina scan, or a one-time number generated by a portable “token-generator.” Security is stronger when access requires multiple credentials.
Cryptography	Cryptography is the method of securing data by making it unintelligible to a human or computer. Cryptography is only useful when the intended recipient can reassemble the data into a readable form using a method known only to the sender and receiver. See also <i>Encryption</i> .
Cyber-Attack	Any offensive action to break into a computer or system. Cyber-attacks can range from installing spyware on a PC, breaking into a payment system to steal card data, or attempting to break critical infrastructure such as an electric power grid.
Data Breach	A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party. Data breaches may involve card data, personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property, etc.
Default Password	A simple password that comes with new software or hardware. Default passwords (like “admin” or “password” or “123456”) are easily guessed and usually are available via online search. They are intended as a placeholder and offer no real security—and must be changed to a stronger password after installing new software or hardware.
Data Security Essentials (DSE)	Data Security Essentials for Small Merchants is a set of educational resources and an evaluation tool to help merchants simplify their security and reduce risk. DSE is intended as an alternative approach to the PCI DSS Self-Assessment Questionnaires (SAQs) for those merchants designated as eligible by the payment brands and their acquirers (merchant banks).
Electronic Cash Register (ECR)	A device that registers and calculates transactions and may print out receipts, but does not accept customer card payments. Also called a “till.”
Encryption	Process of using cryptography to mathematically convert information into a form unusable except to holders of a specific digital key. Use of encryption protects information by devaluing it to criminals. See also <i>Cryptography</i> .
Firewall *	Hardware and/or software that protects network resources from unauthorized access. A firewall permits or denies communication between computers or networks with different security levels based upon a set of rules and other criteria.

Glossary

TERM	DEFINITION
Forensic Investigator	PCI Forensic Investigators (PFIs) are companies approved by the PCI Council to help determine when and how a card data breach occurred. They perform investigations within the financial industry using proven investigative methodologies and tools. They also work with law enforcement to support stakeholders with any resulting criminal investigations.
Hacker	A person or organization that attempts to circumvent security measures of computer systems to gain control and access. Usually this is done in an effort to steal card data.
Hosting Provider *	Offers various services to merchants and other service providers, where their customers' data is "hosted" or resident on the provider's servers. Typical services include shared space for multiple merchants on a server, providing a dedicated server for one merchant, or web apps such as a website with "shopping cart" options.
Integrated Payment Terminal	A payment terminal and electronic cash register in one device that takes payments, registers and calculates transactions, and prints receipts.
Integrator/Reseller	An integrator/reseller is a company that merchants work with to help set up their payment system. This may include installation, configuration, and support. These companies may also sell the payment devices or applications as part of their service. See also <i>Qualified Integrator Reseller (QIR)</i> .
Log *	A file that is created automatically when certain predefined (often security-related) events occur within a computer system or network. Log data includes date/time stamp, description of the event, and information unique to that event. These files are useful for troubleshooting technical issues or a data breach investigation. Also called an "audit log" or "audit trail."
Malware *	Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during many business-approved activities such as via email or browsing websites. Malware examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Merchant Bank *	A bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Also called an "acquirer," "acquiring bank," "card processor," or "payment processor." See also <i>Payment Processor</i> .
Mobile Device	Devices such as smart phones and tablets that are small, portable, and can connect to computer networks wirelessly.
Mobile Payment Acceptance	Using a mobile device to accept and process payment transactions. The mobile device is usually paired with a commercially available card-reader accessory.

Glossary

TERM	DEFINITION
Multi-factor Authentication *	Method of authenticating a user when two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
Network *	Two or more computers connected via physical or wireless means.
Operating System *	Software on a computer system that provides overall management and coordination of computer activities. Examples include Microsoft Windows, Apple OSX, iOS, Android, Linux, and UNIX.
P2PE	Acronym for the PCI Security Standards Council's Point-to-Point-Encryption standard. See details at www.pcisecuritystandards.org .
PA-DSS *	Acronym for the PCI Security Standards Council's Payment Application Data Security Standard. See details at www.pcisecuritystandards.org .
Password *	A word, phrase, or string of characters used to authenticate a user. When combined with the username, the password is intended to prove the identity of the user for access to computer resources.
Patch *	Update to existing software that adds functionality or corrects a defect (or "bug").
Payment Application *	Related to PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement of payment transactions.
Payment Application Vendor	Vendor that sells applications that store, process, and/or transmit card data during payment transactions.
Payment Middleware	A general term for software that connects two or more, perhaps unrelated, payment applications together. For example, it may pass card data between an application on a payment terminal and other merchant systems that send card data to a processor.
Payment Processor *	Entity engaged by merchants to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers (merchant banks) unless defined as such by a payment card brand. Also called a "payment gateway" or "payment service provider" (PSP). See also <i>Merchant Bank</i> .
Payment System	Encompasses the entire process for accepting card payments in a merchant retail location (including stores/shops and e-commerce storefronts) and may include a payment terminal, an electronic cash register, other devices or systems connected to the payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to a merchant bank.

Glossary

TERM	DEFINITION
Payment System Vendor	A vendor who sells, licenses, or distributes a complete payment solution to a merchant. The solution encompasses the hardware and software needed to handle payments within the store and provides a method to connect to a payment processor.
Payment Terminal	Hardware device used to accept customer card payments via swipe, dip, insert, or tap. Also called "point-of-sale (POS) terminal," "credit card machine," or "PDQ terminal."
PCI *	Acronym for Payment Card Industry.
PCI DSS *	Acronym for the PCI Council's "Payment Card Industry Data Security Standard." See details at www.pcisecuritystandards.org .
PCI DSS Compliant	Meeting all applicable requirements of the current PCI DSS, on a continuous basis via a business-as-usual approach. Compliance is assessed and validated at a single point in time; however, it is up to each merchant to continuously follow the requirements in order to provide strong security. Merchant banks and/or the payment brands may have requirements for formal annual validation of PCI DSS compliance.
PCI DSS Validated	Providing proof that all applicable PCI DSS requirements are met at a single point in time. Depending on specific merchant bank and/or payment brand requirements, validation can be achieved through the applicable PCI DSS Self-Assessment Questionnaire or by a Report on Compliance resulting from an onsite assessment.
PCI Validated Payment Application	Software application that has been validated per the PCI Payment Application Data Security Standard (PA-DSS) and is listed on the PCI Council website.
PCI-Approved Payment Terminal	Payment terminal that has been approved per the PCI PIN Transaction Security (PTS) standard and is listed on the PCI Council website.
PCI-Listed Point-to-Point Encryption Solution	Encryption solution that has been validated per the PCI Point-to-Point-Encryption (P2PE) standard and is listed on the PCI Council website.
PED *	Acronym for "PIN entry device." Keypad into which the customer enters their PIN. Also called a "PIN pad."
PIN *	Acronym for "personal identification number." A unique number known only to the user and a system to authenticate the user to the system. Typical PINs are used for automated teller machines for cash advance transactions, or for EMV chip cards to replace a cardholder's signature. PINs help determine whether a cardholder is authorized to use the card and to prevent its unauthorized use if the card is stolen.
Primary account number (PAN) *	Unique number for credit and debit cards that identifies the cardholder account.

Glossary

TERM	DEFINITION
Privilege Abuse	Using computer system access privileges in an abusive manner. Examples include a system administrator accessing card data for malicious purposes, or someone stealing and using an administrator's elevated access privileges for malicious purposes.
PTS *	Acronym for the PCI Council's PIN Transaction Security standard. PTS is a set of modular evaluation requirements for PIN acceptance point-of-interaction (POI) terminals. See details at www.pcisecuritystandards.org .
QIR *	Acronym for "Qualified Integrator or Reseller." QIRs are integrators and resellers specially trained by the PCI Security Standards Council to address critical security controls when installing merchant payment systems. See details at www.pcisecuritystandards.org .
Qualified Security Assessor (QSA) *	A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.
Recurring Payment	A billing method where merchants bill their customers repeatedly over time, such as for monthly memberships or subscriptions. A secure way to do this is for the acquirer/processor to tokenize the card data, which ensures its protection and relieves the merchant from this responsibility.
Remote Access *	Access to a computer network from a location outside of that network. Remote access connections can originate either from inside the company's own network or from a remote location. An example of technology for remote access is a virtual private network (VPN). Remote access can be either internal (e.g. IT support) or external (e.g., service providers, third-party agents, integrators/resellers).
Reseller / Integrator *	An entity that sells and/or integrates payment applications but does not develop them.
Router *	Hardware or software that connects two or more internal or external computer networks to "route" or guide data through a network, and to ensure the data flows properly between those networks. The router can also create more security by permitting only approved traffic and denying unapproved traffic.
Secure Card Reader (SCR)	A PTS-approved device that attaches to a mobile phone or tablet for securely accepting payment cards. PCI PTS-approved SCRs protect and encrypt the card data via SRED. See also <i>SRED</i> .
Security Code *	A three- or four-digit value printed onto the front or back signature panel of a payment card. This code is uniquely associated with an individual card and is used as an additional check to ensure that the card is in possession of the legitimate cardholder, typically during a card-not-present transaction. Also referred to as card security code.

Glossary

TERM	DEFINITION
Self-Assessment Questionnaire (SAQ) *	A questionnaire covering a set of PCI DSS requirements that is completed by the organization itself to confirm it is meeting those requirements.
Sensitive Authentication Data *	Security-related information used to authenticate cardholders and/or authorize payment card transactions, stored on the card's magnetic stripe or chip.
Service Provider *	A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services. Also called a "vendor."
Skimming	Stealing card data directly from the consumer's payment card or from the payment infrastructure at a merchant location such as with an unauthorized hand-held card reader or via modifications made to the merchant's payment terminal. Its purpose is to commit fraud, the threat is serious, and it can hit any merchant's environment.
Skimming Device	A physical device, often attached to a card-reading device, designed to illegally capture and/or store the information from a payment card. Also called a "card skimmer."
Small Merchant	A small merchant is typically an independently owned and operated business with a single location or a few locations, and with limited or no IT budget and often with no IT personnel. Whether a small merchant is required to validate PCI compliance is determined by the payment brand or acquirer (merchant bank).
SRED	An acronym for "Secure Reading and Exchange of Data." A set of PCI PTS requirements designed to protect and encrypt card data in payment terminals. A PCI Council-listed Point-to-Point Encryption (P2PE) solution must use a PTS-approved and listed payment terminal with SRED enabled and actively performing card data encryption.
Stand-Alone Terminal	A payment terminal that does not rely on connection to any other device within the merchant environment and performs no other functions. The only requirement for it to operate is a connection to the processor through either an Internet connection or a telephone line. If the terminal requires connection to a computerized electronic cash register or is multi-function (like a mobile device), it is not a stand-alone terminal.
Strong Authentication	Used to verify the identity of a user or device to ensure the security of the system it protects. The term strong authentication often means with multifactor authentication (MFA).
Till	See <i>Electronic Cash Register</i> .

Glossary

TERM	DEFINITION
Tokenization	A process by which the primary account number (PAN) is replaced with an alternative value called a token. Tokens can be used in place of the original PAN to perform functions when the card is absent like voids, refunds, or recurring billing. Tokens also provide more security if stolen because they are unusable and thus have no value to a criminal.
Unencrypted Data	Any data that is readable without the need to decrypt it first. Also called “plaintext” and “clear-text” data.
Vendor	A business entity that supplies a merchant with a product or service needed for the course of business. Where services are offered, the vendor may be considered a service provider and may require access to physical locations or computer systems within the merchant environment that could affect the security of card data. See also <i>Service Provider</i> .
Virtual Payment Terminal *	Web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. The merchant manually enters payment card data via the securely connected web browser. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtual Private Network (VPN) *	Software that creates a secure, private channel for exchanging data and conducting phone calls over the Internet.
Virus	Malware that replicates copies of itself into other software or data files on an “infected” computer. Upon replication, the virus may execute a malicious payload, such as deleting all data on the computer. A virus may lie dormant and execute its payload later, or it may never trigger a malicious action. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is called a “worm.”
Vulnerability *	Flaw or weakness which, if abused, may result in an intentional or unintentional compromise of a system.
Vulnerability Scan	A software tool that detects and classifies potential weak points (vulnerabilities) on a computer or network. A quarterly external vulnerability scan per PCI DSS Requirement 11.2.2 must be performed by an Approved Scanning Vendor. Other vulnerability scans (such as internal scans and those performed after network changes) can be conducted by qualified staff in an organization’s IT department or by a security service provider (such as an Approved Scanning Vendor). See also <i>Approved Scanning Vendor (ASV)</i> .
Wi-Fi *	Wireless network that connects computers without a physical connection to wires.
Wireless Payment Terminal	Payment terminal that connects to the Internet using any of various wireless technologies.