GUC INFORMATION TECHNOLOGY CONTRACT PROVISIONS

In accepting this Order ("Order"), your company (the "VENDOR"), acknowledges and agrees to abide by the Terms and Conditions set forth below. In the event that a binding written contract signed by both the VENDOR and Greenville Utilities Commission of the City of Greenville (GUC) exists, the terms and conditions of this agreement shall supersede any conflicting terms and conditions of the aforementioned contract.

1. INFORMATION SECURITY

1.1 VENDOR agrees to ensure its software and services comply with all applicable laws and regulations. VENDOR shall, at no additional charge, promptly furnish any updates to the software and services necessary for compliance with any changes in laws or regulations during the terms of this Agreement.

1.2 GUC may, at its expense and for reasonable grounds, require VENDOR to participate in audits and tests relative to GUC and/or services provided by VENDOR on behalf of the GUC.

1.3 VENDOR will take every reasonable precaution to ensure the services and software do not introduce nor contain any virus or similar code that may destroy, modify, alter or cause destruction, modification, or alteration in whole or in part, of any GUC data, equipment, networks, software or utility infrastructure.

1.4 VENDOR agrees to allow GUC access to system security logs that affect this contract, its data, and/or its processes. The VENDOR must provide self-service log reporting or review option, or the VENDOR must produce logs based on regulatory retention requirements of data held (e.g. PCI, HIPAA, etc.)

1.5 The parties agree that the vendor will provide certain services to, for, or on behalf of GUC involving the use or disclosure of Protected Health Information (PHI), as that term is defined by the Health Insurance Portability and Accountability Act (HIPAA). As such, the parties agree to the attached Business Associate Agreement.

1.6 Notification of security incident or data breach: GUC requires notification of event no later than twenty-four (24) hours after initial identification by VENDOR, when any data protection is compromised, or security incident occurs which may impact GUC. Unauthorized access or disclosure of non-public data is considered a breach. The VENDOR will provide notification to the GUC as soon as it is aware of the breach. If the VENDOR is liable for the loss, the VENDOR shall bear all costs associated with the investigation, response, and recovery from the breach. The breach must be communicated to GUC Information Security Officer (ISO).

1.7 Notification of confirmed security vulnerabilities: GUC requires notification within a risk-informed timeframe based on the Common Vulnerability Scoring System (CVSS) or mutually agreeable alternate process. These timeframes are as follows:

i. Critical (9.0-10.0) - twenty-four (24) hours after initial identification by VENDOR
ii. High (7.0-8.9) - forty-eight (48) hours after initial identification by VENDOR
iii. Medium (4.0-6.9) - seventy-two (72) hours after initial identification by VENDOR
iv. Low (0.1-3.9) - seventy-two (72) hours after initial identification by VENDOR

1.8 Prior to the effective date of this agreement, VENDOR will, at its expense conduct or certify that the following certifications have been performed:

i. Attestation under HIPAA, PCI, DSS and/or FedRAMP (NIST, FIPS 200 and SP800-53, ISO 27001, SOC), where applicable
ii. A SOC 2 audit of VENDORS security policies, procedures and controls, to be reviewed and assessed by GUC or its agent, or complete a GUC provided security assessment. The SOC 2 and/or security assessment must report on security controls of the solution/application and/or services to be provided.

iii. A vulnerability scan performed by a third-party service of VENDOR systems under this agreement.

iv. A formal penetration test performed by a process and qualified personnel of VENDOR systems under this agreement.

v. VENDOR will provide GUC the reports or other documentation resulting from the above audits, certifications, scans and tests within thirty (30) calendar days of VENDOR's receipt of such results. Based on the results of the above audits, certifications, scans and tests, VENDOR will, if the results require, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligation under this Agreement and provide GUC with written evidence of remediation.

vi. GUC may, at its expense and reasonable grounds, require VENDOR to perform additional audits and tests within a mutually agreeable timeframe not to exceed thirty (30) calendar days, the results of which will be provided to GUC within seven (7) business days of VENDOR's receipt of results.

vii. VENDOR shall protect GUC data against deterioration or degradation of data quality and authenticity, including, but not limited to, annual third-party data integrity audits performed by an independent, external organization to determine the VENDOR's compliance with standards

1.9 VENDOR agrees to allow GUC (or a designated third-party selected by GUC) the opportunity to perform an onsite inspection of the VENDOR's infrastructure and security practices on an annual basis.

1.10 GUC reserves the right to review the infrastructure and security specifications of the VENDOR in written format on an annual basis.

2. NETWORK SECURITY

2.1 VENDOR agrees at all times to maintain network security that, at a minimum, includes network firewall provisioning, intrusion detection, and regular third-party vulnerability assessments. Likewise, VENDOR agrees to maintain network security that conforms to generally recognized industry standards and best practices that VENDOR then applies to its own network.

3. INTEGRATION & SINGLE SIGN ON

3.1 The application must integrate with Azure Active Directory (Azure ID/Entra ID) using Security Assertion Mark-up Language (SAML), or other industry standard authentication technology as pre-approved by GUC, to provide authentication and single sign on (SSO) services. GUC and VENDOR will exchange the necessary information to configure and test (SSO) prior to implementation in the production environment.

4. USER AUTHENTICATION AND ACCESS RIGHTS

4.1 All facilities used to store, and process GUC data will implement and maintain administrative, physical, technical and procedural safeguards and industry best practices at a level sufficient to secure such data from unauthorized access, destruction, use, modification or discloser. Such measures will be no less protective than those used to secure the VENDOR's own data of a similar type, and in no event less than, for data of the same type and nature, during the term of this Agreement.

4.2 The VENDOR must take the same care to prevent the disclosure of GUC’s confidential information as it takes to prevent disclosure of its own information of a similar nature. In no event, may the VENDOR take less than a reasonable degree of care.

4.3 VENDOR warrants that all GUC data will be encrypted in transmission and at rest (including via web interface).

4.4 ADA Accessibility: VENDOR warrants all digital and interactive content will meet or exceed Web Content Accessibility Guidelines (WCAG) 2.0 A and WCAG 2.0 AA conformance standards, published by the World Wide Web Consortium (W3C), Web Accessibility Initiative (WAI), the organization responsible for developing internet standards. Web accessibility means that people with disabilities can fully and equally perceive, understand, navigate, and interact with the Web as their non-disabled counterparts.

DATA LOCATION

4.5 GUC data, all backups shall not be located, accessed, processed or stored outside of the contiguous United States.

5. ACCEPTABLE USE

5.1 Confidential Information of the other party may be used by the receiving party only about the performance of or as specifically authorized by this Agreement. Each party will protect the confidentiality of Confidential Information of the other party in the same manner that it protects the confidentiality of its own proprietary and confidential information, including, without limitation, by entering appropriate confidentiality agreements with employees, affiliates, independent contractors and subcontractors. Access to Confidential Information will be restricted to the VENDOR's, its personnel (as well as its agents and independent contractors) engaged in a use permitted under this Agreement. Confidential Information may not be copied or reproduced without the disclosing party's prior written consent, except as necessary for use about this Agreement.

5.2 GUC data cannot be used or modified outside of the terms of this agreement without written consent of those actions to be performed.

5.3 Subject to the provisions governing all Confidential Information made available under this Agreement, including copies thereof, will be returned or certified destroyed upon the termination of this Agreement or immediately upon the other party's request; provided, that, subject to the terms of this Section, each party may retain copies of the other party's Confidential Information required for its compliance with its record keeping or quality assurance requirements.

6. PUBLIC RECORDS

6.1 Notwithstanding anything contained herein to the contrary, the parties recognize and acknowledge that GUC is a subdivision of the State of North Carolina and is, therefore, subject to the North Carolina Public Records Act (the "Act") at N.C. Gen. Stat. 132-1 et seq. The parties further acknowledge that any information that is not otherwise protected by law is a public record under North Carolina law and may be released and disclosed GUC pursuant to the Act, and that any such release or disclosure shall not in any way constitute a breach of this Agreement, nor shall GUC be liable to the VENDOR for such release or disclosure. In the event GUC receives a request for disclosure of Confidential Information which the VENDOR has specifically marked "Confidential" or "Proprietary" GUC shall give the VENDOR written notice of such request (the "Notice of Request for Disclosure"). In the event the VENDOR has a reasonable basis for contending that the disclosure of such Confidential Information is not required by the Act, the VENDOR shall within ten (10) calendar days after receipt of the Notice of Request for Disclosure notify GUC in writing of its objection to disclosure and the basis therefor. The VENDOR shall indemnify, defend and hold harmless GUC from and against all losses, damages, liabilities, costs, obligations and expenses (including reasonable attorneys' fees) incurred by GUC

in connection with any refusal by GUC to disclose Confidential Information after receiving an objection to disclosure from the VENDOR. If GUC receives no written objection from the VENDOR within ten (10) calendar days after the VENDOR's receipt of a Notice of Request for Disclosure, GUC shall disclose the Confidential Information referenced in the Notice of Request for Disclosure. Notwithstanding the foregoing, the parties agree that the computer database information that GUC is required to disclose under N.C. Gen. Stat. §132-6.1 shall not be deemed Confidential Information, and that GUC shall be entitled to disclose such information without notice to the VENDOR.

6.2 In accordance with the North Carolina electronic data-processing records law N.C.G.S. §132-6-1, all software and documentation provided by the VENDOR or its subcontractors is subject to potential public inspection and examination.

6.3 All Software and Documentation provided by the VENDOR or its subcontractors will have sufficient information to enable GUC to create an index containing the following information with respect to each database used by the System without extraordinary commitments of staff or resources: (i) annotated list of data fields: name, description, and restricted field indicator; (ii) description of the format or record layout; (iii) frequency with which the database is updated; (iv) list of any data fields to which public access is restricted; (v) description of each form in which the database can be copied or reproduced; (vi) title of the database; (vii) owner of the data; (viii) narrative description of the database; (ix) person creating the index; and (x) purpose of the database. The VENDOR agrees that the GUC may copy and disclose the information listed above in response to requests for database information under the North Carolina General Statutes. (f) All Documentation for the Products and the System is and will be in all material respects complete and accurate, and will enable data processing professionals and other GUC employees with ordinary skills and experience to utilize the Products and the System for the expressed purpose for which they are being acquired by GUC.

7. DATA RETENTION AND DELETION

7.1 Any data entered, loaded and stored in the software are property of GUC. The VENDOR shall provide the GUC a copy of its data for any reason, and at the termination of the services, at no cost to the GUC.

7.2 In the event of an emergency or time-sensitive situation, the VENDOR shall provide GUC the ability to completely retrieve the data from the cloud within twenty-four (24) hours.

7.3 RETURN OF CONFIDENTIAL INFORMATION: The VENDOR will return or destroy GUC's confidential information in all forms and types of media and provide written confirmation or certification of such destruction within thirty (30) calendar days. If the data is returned to GUC, the VENDOR shall provide the data in the file format agreeable to GUC.

7.4 RECORDS RETENTION: To ensure compliance with data retention schedules, the VENDOR will retain data according to retention schedules specified and shall return or destroy GUC's records as requested when allowed by law.

8. BUSINESS CONTINUITY

8.1 VENDOR must provide documented evidence of disaster recovery and business continuity plans. Such plans shall be made available to GUC's upon request for inspection of documentation. If documentation is unavailable, or has not addressed findings in a timely manner, the VENDOR shall be assessed a penalty, up to termination of agreement, for failure in complying with GUC's minimum requirements, as discovered through inspections, audits, or actual disasters.

8.2 VENDOR agrees that any and all data stored, processed, or maintained for GUC will be backed up to a geographically diverse location at a minimum of once per day. VENDOR agrees to provide

certification of successful disaster recovery testing upon request of GUC.

9. WARRANTY

9.1 VENDOR warrants that during the warranty period product and services will be provided according to industry standards.

9.2 VENDOR warrants to GUC that during the applicable warranty period software and services will conform to the operation in accordance with the documentation in all material respects; and services will be carried out according to industry standards in a professional workmanlike manner by qualified personnel.

10. THIRD PARTY VENDORS

10.1 The VENDOR shall inform GUC of any outsourced functionality and its VENDOR.

10.2 Unless otherwise stated within this agreement, no assignment of the contract or components of the contract can occur without explicit, written agreement from GUC. If portions of the service are provided by a third party, the VENDOR is directly responsible for all terms of the contract, regardless of outsourced functions.

11. EXIT

12.1 VENDOR further agrees that following successful transmission of all data to GUC, any and all GUC data will be erased, destroyed, and rendered unrecoverable and certify in writing that these actions have been completed within thirty (30) calendar days of the termination of this Agreement. At a minimum, a "clear" media sanitization is to be performed in accordance to standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization. During the period between termination of the Agreement and authorization for destruction, all security measures must remain intact, including, but not limited to, encryption, backup, and storage.

12. INSURANCE

13.1 Coverage – During the term of the contract, the VENDOR at its sole cost and expense shall provide commercial insurance of such type and with the following coverage and limits:

13.1.1 Workers' Compensation – The VENDOR shall provide and maintain Workers' Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of $1,000,000 each accident, covering all VENDOR's employees who are engaged in any work under the contract. If any work is sublet, the VENDOR shall require the subcontractor to provide the same coverage for any of its employees engaged in any work under the contract.

13.1.2 General Liability – The VENDOR shall provide and maintain Commercial Liability Coverage written on an "occurrence" basis in the minimum amount of $1,000,000 per occurrence.

13.1.3 Automobile – The VENDOR shall provide and maintain Automobile Liability Insurance, to include coverage for all owned, hired, and non-owned vehicles used in connection the contract with a minimum combined single limit of $1,000,000 per accident.

13.1.3 Network security & Privacy Liability (Cyber) The VENDOR shall maintain cyber liability insurance with limits of $3,000,000 per occurrence, providing protection against liability for: (1) privacy breaches (including liability arising from the loss or disclosure of confidential information no matter how it occurs); (2) system breach; (3) denial or loss of service; (4) introduction, implantation, or spread of malicious software code; and (5) unauthorized access to or use of computer systems. Cyber liability insurance shall not include any exclusion or restriction for

unencrypted portable devices or other media. VENDOR shall provide evidence of continuation or renewal for a period of two (2) years following termination of the Agreement.

13.2 Requirements - Providing and maintaining adequate insurance coverage is a material obligation of the VENDOR. 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 to do business in North Carolina by the Commissioner of Insurance. The VENDOR shall at all times comply with the terms of such insurance policies and all requirements of the insurer under any of such insurance policies, except as they may conflict with existing North Carolina laws or this 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. With the exception of Network Security & Privacy Liability (Cyber) Insurance, it is agreed that the coverage as stated shall not be canceled or changed until thirty (30) days after written notice of such termination or alteration has been sent by registered mail to GUC's Procurement Manager.