AMENDMENT No. 1
TO THE MASTER AGREEMENT FOR
SECURE DOCUMENT SHREDDING SERVICES

This Amendment No. 1 (this "Amendment") to the Master Agreement Number 20242, is made and entered into as of February 10, 2020 ("Effective Date"), by and between Green Resource Management, Inc. ("Contractor"), and the Iowa Department of Administrative Services (the "Agency").

NOW, THEREFORE, the parties herein acknowledge and agree as follows:

1. Attachment #9 shall be amended to Exhibit A.
2. Except as set forth in this Amendment No. 1, the Contract shall remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the parties have caused this Amendment No. 1 to be executed by their respective duly authorized representatives as of the date set forth above.

GREEN RESOURCE MANAGEMENT INC

By: _____

Name: Nick Loucks

Title: SALES

Dated: 05/05/22

STATE OF IOWA

By: _____

Name: Bobbi Pulley

Title: Purchasing Agent

Dated: May 12, 2022

EXHIBIT A

Iowa Department of Human Services, Bureau of Collections
Confidential Information Safeguarding Provisions

Definition of Confidential Information. The term "Confidential Information" shall include, but not be limited to, the following:

- All individual case information received pursuant to this Contract unless otherwise designated by the Bureau,
- An individual's social security number,
- An individual's residential and mailing addresses,
- An individual's employment information, and
- An individual's financial information.

Prohibitions against the Use and Disclosure of Confidential Information. The Contractor shall not use, handle, transmit, store, or destroy the Confidential Information of applicants or recipients of child support enforcement services in a manner or for any purpose, except as allowed by the provisions of the Contract. The Contractor shall safeguard the confidentiality of Confidential Information concerning applicants or recipients of child support enforcement services according to 5 U.S.C. § 552a; 26 U.S.C.
§ 6103; 42 U.S.C. §§ 654 and 654a; Iowa Code § 252B.9; 45 CFR Parts 303.21 and 307.13; and other applicable federal and state laws.

Internal Revenue Service Data. The Contractor shall adhere to the safeguarding provisions of *Internal Revenue Service Publication 1075*. The **Internal Revenue Service Confidential Information Safeguarding Provisions** contains a summary of the Contractor's Confidential Information safeguarding requirements and penalties pertaining to Internal Revenue Service information.

Reporting. The Contractor shall report to the Bureau's Security and Privacy Officer and the Child Support Recovery Unit any use or disclosure of the Confidential Information not provided for by this Contract of which the Contractor becomes aware, as well as report any suspected or unauthorized access to or disclosure of Confidential Information. The Contractor agrees to report suspected or unauthorized access to or disclosure of Confidential Information immediately, as the Bureau is required to report the suspected or unauthorized access or disclosure within the following timeframes:

- Federal Tax Information .....24 hours
- Social Security Information .....1 hour
- Federal Parent Locator Service .....1 hour
- All other Confidential Information .....3 Business Days

Sanctions. State and federal statutes carry criminal penalty or civil liability for confidentiality violation. For example, see Iowa Code § 252B.10; 5 U.S.C. § 552a; 42 U.S.C. §§ 653(l)(2) and 654a(d)(5); and
26 U.S.C. §§ 7213, 7213A, and 7431. The Contractor may not use the Confidential Information for commercial or political purposes or re-disclose the Confidential Information without the express, written consent of the Bureau. The Contractor may be held civilly or criminally liable for misuse of the Confidential Information.

Survival. The provisions of the Contract that protect Confidential Information shall survive termination of the Contract.

Rev. 4/14/22

Internal Revenue Service Confidential Information Safeguarding Provisions

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the Contractor.

(2) The Contractor and Contractor's officers or employees, as well as any Subcontractor or Subcontractor's officers or employees, to be authorized access to federal tax information (FTI) must meet background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the CSRU and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The Contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, civil and criminal penalties, and obligations of this contract apply to performing services with FTI, the Contractor shall assume toward the Subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the Contractor, and the Subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the agency under this contract.

(11) In addition to the Subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the Subcontractor, and the Subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and obligated to the agency under this contract. The Subcontractor is hereby notified that any civil and criminal penalties set forth herein for unauthorized access, disclosure or use of confidential information are equally applicable to the Subcontractor and its officers and employees.

(12) For purposes of this contract, the term "Contractor" includes any individual, organization or business contractor, and any officer or employee of the individual, organization or business Contractor who has access to or who uses FTI, and the

term "Subcontractor" includes any individual, organization, or business subcontractor, and any officer or employee of the individual, organization or business subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1(c).

(4) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(5) Granting a Contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A Contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.