

CONTRACT ROUTING FORM

1. Complete the information below BEFORE printing and completing items 2 through 7. Items in red are required.

Department: Tax

Department contract file name (use effective date): North Carolina Wildlife Resources

Commission_Tax_20241001

Project Code: Click here to enter text.

Contract type: MOU/MOA

Contracted Services/Goods: Vessel Information

Contract Component: Master

Change Order Number/Addendum Number: Click here to enter text.

Vendor Name: Click here to enter text.

Effective Date: 10/01/2024

Approved by: County Manager

Date approved by the BOC: Click here to enter text.

Ending Date: Click here to enter a date.

Total Amount: not applicable

Please Return Contract to:

Name: Jenny Williams

Email:

jenny.williams@chathamcountync.g

ov

Special Instructions for Clerks

Office:

2. Department Head or his/her designee has read the contract in its entirety.

By: Jenny Williams (Department Head signature required)

3. County Attorney has reviewed and approved the contract

County Attorney has reviewed and rejects the contract Reason: _____

This is an automatic renewal and does not require approval from the County Attorney: Yes No



If this box is checked the County Attorney's Office has reviewed the contract but has not made needed changes to protect the County because the contract is a sole source contract and the services required by the County are not available from another vendor.

4. Technical/MIS Advisor has reviewed the contract if applicable. Yes No

5. Vendor has signed the contract. Yes No

6. A budget amendment is necessary before approval. Yes No

If budget amendment is necessary, please attach to this form.

7. Approval

Requires approval by the BOC - contracts over \$100,000.00. Follow Board submission guidelines.

Requires approval by the Manager – contracts \$100,000 or less.

8. Submit to Clerk.

Clerk's Office Only

Finance Officer has signed the contract

The Finance Officer is not required to sign the contract

Jenny Williams

From: Christy Blackburn
Sent: Wednesday, September 18, 2024 2:26 PM
To: Jenny Williams
Subject: FW: NC Wildlife Vessel Tax MOA
Attachments: NCWildlilfe_MOA.pdf

Bob approved, now what do I need to do?

Best Regards,
Christy

Christy Blackburn

Tax Listing Supervisor
Chatham County Government
christy.blackburn@chathamcountync.gov
919-545-8475 (Phone) | 919-542-2963 (Fax)
www.chathamcountync.gov
12 East Street | PO Box 908
Pittsboro, NC 27312

In keeping with the NC Public Records Law, e-mails, including attachments, may be released to others upon request for inspection and copying.

From: Ann Hammack <ann.hammack@chathamcountync.gov>
Sent: Wednesday, September 18, 2024 11:56 AM
To: Christy Blackburn <christy.blackburn@chathamcountync.gov>
Subject: NC Wildlife Vessel Tax MOA

Christy,

Bob has approved the attached.

Ann Hammack

County Paralegal
Chatham County Government
County Manager's Office
Email: Ann.Hammack@chathamcountync.gov
919-545-8308 (Phone) | 919-542-8272 (Fax)
Chathamcountync.gov
12 East Street | P.O. Box 1809
Pittsboro, NC 27312

In keeping with the NC Public Records Law, e-mails, including attachments, may be released to others upon request for inspection and copying.

MEMORANDUM OF AGREEMENT

NORTH CAROLINA WILDLIFE RESOURCES COMMISSION

AND

Chatham County, NC

THIS AGREEMENT is made and entered into on the last date executed below, by and between the NORTH CAROLINA WILDLIFE RESOURCES COMMISSION, hereinafter referred to as "NCWRC," and Chatham County, NC, hereinafter referred to as "Vessel Tax County," referred to collectively as "the Parties."

WITNESSETH

WHEREAS, NCWRC is a government agency of the State of North Carolina that works to protect, conserve and restore North Carolina's wildlife and habitat.

WHEREAS, the Vessel Tax County is a local government entity of the State that collects tax on vessels from citizens.

WHEREAS, in order for the Vessel Tax County to determine the tax of vessels and notify the citizens of the tax, the Vessel Tax County needs information, including Personal Identifying Information held by NCWRC;

WHEREAS, NCWRC is not authorized to disclose "Personal Identifying Information" except in certain circumstances, including but not limited to, if the Personal Identifying Information is "disclosed to another governmental entity or its agents, employees, or contractors if disclosure is necessary for the receiving entity to perform its duties and responsibilities. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of such numbers." N.C.G.S. §132-1.10 (b)(5).

NOW, THEREFORE, the Parties, each in consideration of the promises and undertakings of the other as herein provided, do hereby covenant, and agree, each with the other, to the following:

The Vessel Tax County agrees that:

1. The Vessel Tax County is requesting information from NCWRC that includes "Personal Identify Information," as defined by N.C.G.S. 14-113.20(b). The "Personal Identifying Information" requested by the Vessel Tax County from NCWRC includes: OwnerName | Phone | MailAddr1 | MailAddr2 | MailCity | MailState | MailZip | MailZip4 | MailCounty | ResAddr1 | ResAddr2 | ResCity | ResState | ResZip | ResZip4 | ResCounty | TaxCounty.

2. By signing this Agreement, the Vessel Tax County certifies that it is a governmental entity, and disclosure of the requested Personal Identifying Information is necessary for the Vessel Tax County to perform its duties and responsibilities.
3. The Vessel Tax County shall maintain the confidential and exempt status of any Personal Identifying Information provided to it under this Agreement.
4. The Vessel Tax County is only authorized to use the Personal Identifying Information provided by NCWRC to determine vessel property tax values and to notify vessel owners of the tax.
5. The password(s) provided to the Vessel Tax County for downloading vessel data and accessing Go Outdoors NC shall not be shared.
6. The Vessel Tax County shall not release or disclose Personal Identifying Information to any third party for any reason, except as authorized by law.
7. The Vessel Tax County 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 this Agreement, including those of federal, state, and local agencies having jurisdiction and/or authority.
8. The Vessel Tax County shall notify NCWRC of any security breaches within 24 hours as required by G.S. 143B-1379. For further information, see, G.S. 75-60 et seq.
9. The Vessel Tax County shall comply with the NC Department of Information Technology (DIT) requirements relating to the security of the State network, and rules relating to the use of the State network, IT software and equipment. See, e.g., G.S. 143B-1376.

9. GENERAL INDEMNITY:

(a) The Vessel Tax County shall indemnify, defend and hold and save NCWRC, 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 also from any and all claims and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Vessel Tax County in the performance of this Agreement that are attributable to the negligence or intentionally tortious acts of the Vessel Tax County, provided that the Vessel Tax County is notified in writing within 30 days from the date that NCWRC has knowledge of such claims.

b) The Vessel Tax County, at its own expense, shall defend any action brought against NCWRC under this section. The Vessel Tax County 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 NCWRC shall have the option to participate in such action at its own expense.

c) The Vessel Tax County represents and warrants that it shall make no claim of any kind or nature against NCWRC agents who are involved in the delivery or processing of the information provided herein or Services as part of this Agreement with NCWRC.

10. CARE OF NCWRC DATA AND PROPERTY: Any NCWRC property, information, data, instruments, documents, studies or reports given to or prepared or assembled by or provided to the Vessel Tax County under this Agreement shall be kept as confidential, used only for the purpose(s) required to perform this Agreement and not divulged or made available to any individual or organization except as authorized by law.

11. NCWRC data and property in the hands of the Vessel Tax County shall be protected from unauthorized disclosure, loss, damage, destruction by a natural event or another eventuality. The Vessel Tax County agrees to reimburse NCWRC for loss or damage of NCWRC property while in the Vessel Tax County's custody. Such data shall be destroyed or returned to NCWRC in a form acceptable to NCWRC upon the termination or expiration of this Agreement.

12. Storage, sharing, destruction and sanitization of this vessel data must be as provided in accordance with the following NCDIT specifications. [NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information](#)

[SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\) | CSRC \(nist.gov\)](#)

[Handbook for Safeguarding Sensitive Personally Identifiable Information | Homeland Security \(dhs.gov\)](#)

[NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization](#)

13. The Vessel Tax County shall make their storage of the vessel data available for inspection by NCWRC or its representatives' inspection at any time.

14. The Vessel Tax County shall ensure vessel tax county data shared with a contractor or 3rd party vendor are agreeing to the following SECURITY OF STATE DATA rules and Policy:

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

back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.

- e) The Vendor shall certify to the State:
- i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.

- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems

reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. 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 the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and also in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - 1) The scale and quantity of the State Data loss;
 - 2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - 3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.

- 4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

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

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

WRC agrees that:

15. It shall provide the requested information to the Vessel Tax County, annually, via access to a computer program. The computer program will be accessed using a password provided to the Vessel Tax County.

16. It shall refresh the Vessel data in the computer program twice annually.

17. It shall provide the Vessel Tax County with any password changes in a timely manner.

18. It shall provide real time read-only access to vessel data and reports through the Go Outdoors NC (GONC) application.

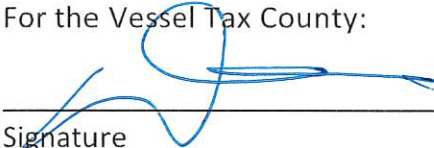
The Parties agrees that:

19. NCWRC shall have the authority to remove the Vessel Tax County Application's access at its discretion.
20. This Agreement shall be effective from the execution date below until Oct 1, 2024.
21. SITUS AND GOVERNING LAWS: This Agreement is made under and shall be governed by and construed in accordance with the laws of the State of North Carolina, including, without limitation, the relevant provisions of G.S. Chapter 143, Article 3, and the Rules in 01 NCAC Chapter 05, and any applicable successor provisions, without regard to its conflict of laws rules, and within which State all matters, whether sounding in Contract, tort or otherwise, relating to its validity, construction, interpretation and enforcement shall be determined.
22. ACCESS TO PERSONS AND RECORDS: During, and after the term hereof during the relevant period required for retention of records by State law (G.S. 121-5, 132-1 et seq., typically five years), the State Auditor and any Purchasing Agency's internal auditors shall have access to persons and records related to this Agreement to verify accounts and data affecting performance under the Agreement, as provided in G.S. 143-49(9). However, if any audit, litigation or other action arising out of or related in any way to this project is commenced before the end of the such retention of records period, the records shall be retained for one (1) year after all issues arising out of the action are finally resolved or until the end of the record retentions period, whichever is later.
23. ENTIRE AGREEMENT: This Agreement represents the entire agreement between the parties and supersedes all prior oral or written statements or agreements. All promises, requirements, terms, conditions, provisions, representations, guarantees, and warranties contained herein shall survive the Agreement expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable Federal or State statutes of limitation.
24. AMENDMENTS: This Agreement may be amended only by a written amendment duly executed by NCWRC and the Vessel Tax County.
25. SOVEREIGN IMMUNITY: Notwithstanding any other term or provision in this Agreement, 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 NCWRC under applicable law.

26. This Agreement is not transferrable or assignable.

Entered into this _____ day of _____, 2024:

For the Vessel Tax County:



Signature

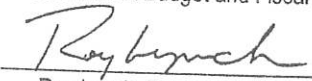
Dan LaMontagne County Manager
Printed Name and Title

For NCWRC:

Signature

Cameron Ingram, Executive Director
Printed Name and Title

This instrument has been pre-audited in the manner required
by the Local Government Budget and Fiscal Control Act.



Roy Lynch, Finance Officer