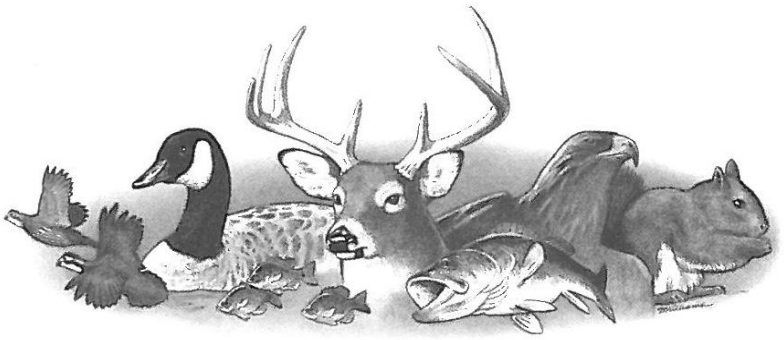

North Carolina Wildlife Resources Commission

M. Kyle Briggs, Executive Director

AGREEMENT FOR USE OF NCWRC HUMAN SUBJECTS DATA

WHEREAS the North Carolina Wildlife Resources Commission, herein referred to as "NCWRC," and INSTITUTION NAME, by and through PI NAME, herein referred to as "INSTITUTION NAME OR ABBREVIATED NAME," share a mutual interest BRIEF SUMMARY OF REASON FOR REQUEST; and

WHEREAS collaborative work is mutually beneficial for all parties to further scientific knowledge and understanding of wildlife management and human subjects;

NOW THEREFORE, based on the mutual benefit likely to result from the shared data, the Parties agree as follows:

It is agreed herein by all Parties that:

1. NCWRC shall provide the data requested in Attachment A, which is attached hereto and specifically incorporated by reference.

2. Data provided by NCWRC shall be handled with high ethical standards and shall only be used for the analysis or project expressly listed in Attachment A.

3. INSTITUTION NAME shall use all reasonable care to safeguard the data provided by NCWRC to ensure the protection of human subjects. Data included under this request shall not be left on public computers or other shared devices, nor copied, provided or distributed in any form, including geographic coordinates, location data, maps, direction, "geotagged" phones, online blogs or forums, or any social media without prior written consent of NCWRC.

4. INSTITUTION NAME shall ensure that no personal identifying information is directly or indirectly linked to responses when using human subjects data.

5. INSTITUTION NAME shall consult NCWRC on matters concerning the interpretation of data provided. If the data are used to produce a report, article, peer-reviewed manuscript, or map, INSTITUTION NAME shall provide NCWRC with a copy of the same for review and approval prior to dissemination. INSTITUTION NAME shall collaborate with NCWRC to produce these materials, if applicable.

Mailing Address: 1701 Mail Service Center, Raleigh, NC 27699-1700
Phone: (919) 707-0010 ◆ Fax: (919) 707-0020

6. Publications and reports that result from the collaboration shall acknowledge FUNDING SOURCE funding, as well as the efforts of NCWRC staff in collecting used data, reviewing research materials and/or participating in the research project.

7. INSTITUTION NAME shall provide NCWRC with a copy of the project's approved Institutional Review Board (IRB) protocols, if applicable.

8. INSTITUTION NAME shall submit electronic files to NCWRC of all raw and processed data collected, including geospatial information and codes used for any subsequent analysis, prior to the conclusion of the project or the publication of results.

9. Additional projects or publications using NCWRC data shall not be pursued without prior written approval, nor shall data requested or generated be shared with a person or organization, without prior written approval from NCWRC.

10. All NCWRC digital data provided under this Agreement, and any copies/versions made from that data, shall be deleted from computer systems within three years from the date the Agreement is fully signed.

11. Storage, sharing, destruction and sanitization of the VIS data provided by NCWRC should be in compliance with best practices as provided in accordance with the following NCDIT specifications:
    - SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) | CSRC
    - Handbook for Safeguarding Sensitive Personally Identifiable Information | Homeland Security
    - NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization | NIST

12. INSTITUTION NAME and its agents and subcontractors shall abide by the following SECURITY OF STATE DATA rules and Policies:
    a. All materials, including software, Data, information and documentation provided by the State to INSTITUTION NAME (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. INSTITUTION NAME shall protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary _____materials shall be identified to the State by INSTITUTION NAME prior to use or provision of Services hereunder and shall remain the property of _____. Derivative works of any _____ proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. INSTITUTION NAME 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 Agreement, or (iv) at State's written request. INSTITUTION NAME 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 INSTITUTION NAME shall be disclosed in any form without the prior written agreement with NCWRC. INSTITUTION NAME will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

b. INSTITUTION NAME shall not store or transfer non-public NCWRC data outside of the United States. This includes backup data and Disaster Recovery locations. INSTITUTION NAME shall permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.

c. INSTITUTION NAME 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-dataclassification-handling-policy/open) that is collected by NCWRC and stored in any _____ site or other _____ housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by INSTITUTION NAME or its agents or subcontractors in connection with the provision of the Services. INSTITUTION NAME 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 NCWRC of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.

d. INSTITUTION NAME shall provide and maintain secure backup of the State Data. INSTITUTION NAME 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 WRC's access to its Data and the Services. INSTITUTION NAME shall allow periodic back-up of NCWRC Data by NCWRC to NCWRC's infrastructure as the State requires or as may be provided by law.

e. INSTITUTION NAME shall certify to the State:

1) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;

2) The system used to provide the services under this Agreement has maintained and shall maintain a valid 3rd party security certification not to exceed 1 year that is consistent with the data classification level and 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.

3) 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) INSTITUTION NAME shall encrypt all non-public data in transit regardless of the transit mechanism.

(b) For engagements where INSTITUTION NAME stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, email addresses, customer numbers, residence addresses, driver's license number, financial data, federal/state tax information, and hashed passwords. INSTITUTION NAME's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. When INSTITUTION NAME cannot offer encryption at rest, it must maintain, for the duration of this Agreement, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, INSTITUTION NAME 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. §§ 143B1376 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 the USCG 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 the USCG 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 INSTITUTION NAME becomes aware of any Security Breach due to its acts or omissions other than in accordance with the terms of the Agreement, INSTITUTION NAME 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. INSTITUTION NAME 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 INSTITUTION NAME's 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.

i. INSTITUTION NAME 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 INSTITUTION NAME 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, INSTITUTION NAME 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 NCWRC.

l. In the event of temporary loss of access to Services, INSTITUTION NAME 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, INSTITUTION NAME 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. INSTITUTION NAME shall provide such notification within twenty-four (24) hours after it reasonably believes there has been such a disaster or catastrophic failure. In the notification, INSTITUTION NAME shall inform the State of:

    1) The scale and quantity of the State Data loss;

    2) What INSTITUTION NAME 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 INSTITUTION NAME has taken or will take to prevent future State Data and Services loss.

    4) If INSTITUTION NAME fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement. INSTITUTION NAME 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. INSTITUTION NAME shall cooperate fully with the State, its agents and law enforcement.

n. In the event of termination of this contract, cessation of business by INSTITUTION NAME or other event preventing INSTITUTION NAME from continuing to

provide the Services, INSTITUTION NAME 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 INSTITUTION NAME's obligation to provide the State Data pursuant to this Paragraph 18) n), INSTITUTION NAME 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, INSTITUTION NAME 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.

13. This Agreement obligates neither party to a duty for or expectation of payment for said services, and each party agrees to individually fund their representative portions of said work unless specifically addressed in further agreements.

14. Nothing in this Agreement shall obligate either party to any conditions not specifically stated herein.

15. This Agreement, its situs and forum, shall be North Carolina, where all matters, whether sounding in contract or tort, relating to its validity, construction, interpretation, and enforcement shall be determined.

16. This Agreement is made under and shall be governed, construed and enforced in accordance with the laws of the State of North Carolina, without regard to its conflict of laws rules.

17. 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 this Agreement to verify accounts and data affecting fees or performance under this Agreement, as provided in G.S. 143-49(9).

18. This Agreement and any documents incorporated specifically by reference represent the entire agreement between the parties and supersede all prior oral or written statements or agreements.

19. This Agreement may be revised as necessary by mutual consent of all parties by the issuance of a written amendment, signed and dated by all parties.

20. 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 that otherwise would be available to NCWRC under applicable law.

21. The failure to enforce or the waiver by NCWRC of any right or an event of breach or default on one occasion or instance shall not constitute the waiver of such right, breach or default on any subsequent occasion or instance.

22. 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.

23. This Agreement shall become effective as soon as it is signed by the parties hereto and run for a period of 3 years, at which time it can be renewed in for periods of an additional 3 years.

24. Either party may terminate this Agreement in whole, or in part, at any time by giving the other party written notice not less than 30 days prior to the effective date of such termination.

_____ _____

NCWRC Authorized Representative Date

_____ _____

INSTITUTION NAME Auth. Rep Date