**Consent Form**

**Understanding perceptions of alternative lobster fishing gear in Maine**

You are invited to participate in a research project being conducted by a team of researchers from the University of Maine (Tracy MacKeracher, PhD Candidate; Kate Behrens, PhD Student,  Dr. Joshua Stoll, Faculty), the Maine Center for Coastal Fisheries (Dr. Alexa Dayton, Executive Director; Dr. Carla Guenther, Chief Scientist, Dr. Molly Miller, Researcher), and Sunrise County Economic Council (Dr. Tora Johnson, Co-Director). The purpose of the research is to understand perceptions of lobster harvesters regarding alternative fishing gear. Lobster permit holders who are over 18 and who fished in 2023 are eligible to participate in this study.

**What Will You Be Asked to Do?** If you decide to participate, you will be asked to take part in a 45-60 25-35 minute in-person oronline survey or phone interviewsurvey on a day, and at a time and place that is convenient for you. During the interview, you will be asked questions to understand your perspectives regarding alternative lobster fishing gear. With your consent, we will use a handheld voice recorder to use software to record your responses to the interview questions. Notes will be taken during the interview if you do not wish for the interview to be audio recorded.

**Risks**: The primary risks are the loss of time and convenience that participating may cause, as well as the remote possibility of a breach of confidentiality. Before beginning the interview, you will be reminded that, at any time, you can (i) end your participation; (ii) take a break; and/or (iii) skip any question(s) that you are not comfortable answering.

**Benefits:** There are no anticipated direct benefits for participating in this study, however we will provide feedback to you and your community about what we discover in our research. This research has the potential to offer important insights to help support the long-term sustainability of lobster fishing for communities in Maine.

**Confidentiality:**

**Data Security and Confidentiality**

The issues of confidentiality and security are central to ensuring the accuracy of the responses. We must respect the privacy of our respondents by protecting their identity. Ensuring the security and confidentially of the survey data starts before we conduct a survey. During the data collection process, all data collected from the online survey will be stored on a secure, encrypted and password protected computer network hosted by Voxco. This data is only accessible by senior researchers who have an administrative account and password used to manage the survey. Voxco offers the highest levels of data security, including Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data.

When responding to the survey, access is limited to those with a valid ID, which ensures only sampled respondents can complete the survey. In addition, because the sample database is integrated, anyone completing the survey online is automatically flagged and removed from receiving any telephone calls.

We are committed to providing absolute confidentiality for all individuals and the highest level of security for sensitive and personal data. Our company respects the privacy of individuals, protects them from abuse and harm, and has put numerous safeguards in place to protect the confidentiality of any data collected from individuals.  We rely on an established set of guidelines that insure confidentiality. These include:

* A comprehensive set of HIPAA compliant data security policies, including appropriate handling of personally identifiable information (PII) and protected health information (PHI).
* Adherence to America Association of Public Opinion Research best practices for the ethics of survey research.
* Use of industry-approved software, such as Microsoft SharePoint, to securely transfer, store, and host all our files, including those that contain confidential data.
* Limiting access to confidential information to senior research staff who require it to complete their work.
* Providing statements of confidentiality and consent to respondents prior to conducting a survey or interview.
* We will under no circumstances release respondent information unless explicit permission is obtained from the respondent

We also believe in maintaining the confidentiality of survey materials, survey results, data, and other information that is purchased by our clients. We treat all research materials, surveys, reports, datasets, and other deliverables as confidential and the property of our clients.  It is our policy to never release information without the express, written approval of our clients.

MDR’s Information Security Program including all information security policies, plans, and agreements is overseen by Nat Mildner, MDR’s Information Security Officer (ISO). The ISO is also responsible for conducting an annual audit of MDR’s Information Security Program policies and procedures to ensure compliance and incorporate appropriate modifications.

**Data Security**

Since 2020 MDR has worked with a managed IT and cybersecurity services firm, Systems Engineering Inc., to review and update our policies and practices surrounding the transfer and storage of confidential information yearly to ensure we follow current best practices and the most up to date National Institute for Standards and Technology (NIST) Cyber Security Framework (CSF). Aligning our policies and practices with the NIST Framework broadly means we use the same underlying standard as most regulatory requirements such as HIPAA.

Starting in 2024 MDR deepened our relationship with Systems Engineering to be our fully managed services provider and be part of their Adaptive Cybersecurity Framework (aCSF) program. Through that program our IT systems are continually monitored and updated to keep them safe from the latest cybersecurity threats.

Our specific methods for file and data storage include:

* All files are stored within MDR’s Microsoft Azure data tenant enterprise level physical security, backup, and redundancy. All data are stored within the U.S.
* All access to MDR electronic systems is controlled via company issued accounts with access tailored by job need with user identity verified through multi-factor authentication at least every 72 hours.
* Each project has a secure folder in a dedicated SharePoint library where sensitive files can be transferred between MDR and the client. Access is limited to the minimum needed staff and any external transfers must be through an authenticated MDR SharePoint sharing link.

We have met the obligations of clients with the most demanding data security standards, including NCQA through our work on the Medicare Health Outcomes Survey.

**Recording: All telephone calls are recorded and stored on Market Decisions Research’s secure drive.**

**Voluntary:** Participation is voluntary, and you can skip any questions you prefer not to answer. You have the option to withdraw during the interview at any point during the conversation. Participating in the interview indicates consent.

**Contact Information:** If you have any questions about this study, please feel free to contact us:

Tracy MacKeracher: tracy.mackeracher@maine.edu, 207-745-2014

Dr. Alexa Dayton: adayton@coastalfisheries.org

Dr. Carla Guenther: cguenther@coastalfisheries.org

Dr. Tora Johnson: tjohnson@sunrisecounty.org

Dr. Joshua Stoll: joshua.stoll@maine.edu

If you have any questions about your rights as a research participant, please contact the Office of Research Compliance, University of Maine, 207-581-2657 (or e-mail umric@maine.edu).