PRIVACY & ACCEPTABLE USE POLICY
(Exhibit C)

0. General

This document constitutes EpiGrid’s Privacy and Acceptable Use Policy, here after referred to as the Policy. The Policy describes and defines Acceptable uses and Activities, Prohibits certain uses and Activities, as well as describes EpiGrid's commitment to the Privacy of Customer information and data. Any Activity or Use of EpiGrid services that are illegal, infringe the rights of others, or interfere with EpiGrid’s services are expressly prohibited.

For the purposes of this Policy the Reseller is defined as and is considered the same as the Customer except as explicitly stated.

The Customer, the Customer's employees, and the Customer's Agents agree to comply with all applicable government and regulatory laws and regulations and this Policy. EpiGrid may suspend or terminate a Customer's service and access to data for failure to comply with this Policy.

1. Privacy

EpiGrid will use the Customer’s personal information only as reasonably necessary to provide contracted services and to collect fees owed and will not disclose such information to any third party except as required by law as evidenced by an order of a court of competent jurisdiction and to collection services if needed. EpiGrid will not use the Customer’s name, business name, or comments in marketing documents without written consent from the Customer. At any time, the Customer can send a written notice to withdraw any consent previously given.

2. Equipment, Data, Software, Network, and Premises

EpiGrid owns and maintains physical equipment for the purpose of providing services. The Customer is granted limited virtual access to portions of the physical equipment according to the type of service being provided. The physical equipment and the limited virtual access to portions of the equipment shall here after be known as Equipment.

The Equipment is physically installed in multiple Data Centers. Each Data Center is defined as the physical and real geographical location where EpiGrid installs and maintains Equipment.

In the course of providing Services to the Customer, EpiGrid may install and/or store Software and Data on the Equipment in accordance with this Policy. Likewise, the Customer is granted limited virtual access to install and/or store Software and Data on the Equipment in accordance with this Policy. Software is defined as a program or algorithm used to access, read, write, or modify the Data. Data is defined as a collection of information stored digitally on the Equipment.

EpiGrid also owns a Network that interconnects all of the EpiGrid Equipment at and between all of the Data Centers. The Network is created, used and maintained in accordance with this Policy to allow virtual access to the Equipment. The Customer is granted limited virtual access to and use of the Network according to this Policy. Digital and Virtual access to the Equipment and Network shall be known as an Account or Customer's Account. The Account may constitute multiple users for which there is a unique password for each. The sum total of a Customer's users and passwords shall be known as an Account or Customer's Account.

The Premises shall be defined as the sum total of the Data Centers, Equipment, Software, Data, and Network.

The Customer has no other rights related to the Premises, Data Centers, Equipment, Software, Data, and Network. Physical access to the Premises, Data Centers, Equipment, Software, Data, and Network by the Customer is strictly prohibited.

3. Immediate Threats

If, in the determination of EpiGrid acting reasonably, the Equipment, Software, Data, or Network used by the Customer or the activities of the Customer poses an immediate threat to the physical integrity of the Premises or the performance of the Equipment and/or Network of EpiGrid or any other Customer accessing of the Premises, or poses an immediate threat to the safety of any person, then EpiGrid may perform such work and take such other actions that it may consider necessary without prior notice to the Customer and without liability for damage to the Equipment, Software, Data, or Network for any interruption of the Customer's (or its Customers') businesses. As soon as practical after performing such work, EpiGrid will advise the EpiGrid Reseller responsible for direct interaction with the Customer, by email, of the work performed or the action taken. The EpiGrid Reseller will be responsible for advising the Customer.

4. Storage and Security

At all times, the Customer bears full risk of loss or breach of security or breach of confidentiality of any Software, Data, or other content, here forward defined as Content, that the Customer places on the EpiGrid Equipment or transmits via the EpiGrid Network. The Customer is entirely responsible for maintaining the confidentiality of the passwords and account information that is used to secure the Customer's Account and access to the Equipment and Network. The Customer acknowledges and agrees that they are solely responsible for all acts, omissions, and use of their Customer Account or in the digital connection with the Network or any of the Content displayed, linked, or transmitted through or stored on the Network and Equipment.

EpiGrid nor the EpiGrid Reseller undertake no obligation to provide management or security services beyond those defined in the Policy unless specifically requested and agreed in an additional Service Level Agreement, defined as an SLA, between EpiGrid, the Reseller, and the Customer. If any technology specifically associated with the Customer's account requires updating, they must make a request for such update through their EpiGrid Reseller.

The Customer shall be solely responsible for undertaking measures to:

a. Prevent any loss or damage to their content.

b. Maintain independent archival and backup copies of their content beyond the agreed scope of services guaranteed by EpiGrid i.e. 7-day backup, 14-day backup, etc.
c. Ensure the security, confidentiality and integrity of their content transmitted through or stored on EpiGrid servers.
d. Ensure compliance with all laws and regulations applicable to data stored.
e. Maintain and provide to EpiGrid updated license/keys for installed software that requires subscription/renewal in a timely manner for software license/keys the customer acquired/provided, EpiGrid shall not be responsible for downtime resulting from a missing or outdated license/key.
f. Using encryption methods for all Content (by a minimum of a 256 bit key encryption) and maintaining strong passphrases as specified by encryption hardware or software standards.

5. Government Access Requests

EpiGrid does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies may use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. EpiGrid's practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of EpiGrid services.

6. Acceptable Use

The Customer’s use of EpiGrid’s Equipment and Network and the use of the Customer's Account is conditioned upon the following:

i. **Prohibited Uses or Actions, Content and Illegal Use**:
Customer may not use EpiGrid services to:

- Engage in, aid, or assist any activity that is in violation of the law or regulation or the rules of an Internet Service Provider;

- Violate, infringe, or misappropriate the privacy rights or property rights of others.

- Send, post, host, or display content that is unlawful, harassing, threatening, abusive, libelous, tortious, invasive of another's privacy, hateful, obscene, harmful to minors in any way or is racially, ethnically, or otherwise objectionable.

- Intentionally omit, delete, forge, or misrepresent transmission information or withhold or cloak identity or contact information.

- Intentionally transmit or otherwise propagate computer viruses or similar destructive computer codes.

- Administer Internet Relay Chat (IRC)

- Upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way, information, software or other material obtained through EpiGrid services or otherwise that infringes any patent, trademark, trade secret or is protected by copyright, nondisclosure agreement, or other propriety right, without obtaining any required permissions of the owner.

- Send very large numbers of copies of the same or substantially similar messages, empty message, or messages which contain no substantive content, or send very large messages or files that disrupt a server, account, newsgroup, or chat service.

- Impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, "phishing").

- Access any other person's computer or computer system, network, software, applications, or data without his or her knowledge and consent; breach the security of another user or system; or attempt to circumvent the user authentication or security of any host, network, or account.

- Use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, including password guessing programs, decoders, password gathers, keystroke loggers, analyzers, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is prohibited.

- Restrict, inhibit, interfere with, or otherwise disrupt or cause performance degradation, regardless of intent, purpose or knowledge, to EpiGrid services.

- Interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host.

- Engage in any other activities that may reasonably be deemed prohibited by EpiGrid for the purposes of safety, privacy, system reliability, protection of equipment, systems, data, and personnel, and compliance with laws or regulations from governmental agencies.

ii. **Commercial Email**:
Customer must comply with the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) which establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask the sender of the email to stop spamming them.

a. The CAN-SPAM Act:
   - Bans false or misleading header information.
   - Prohibits deceptive subject lines.
   - Requires that the sender of the email give recipients an opt-out method.
   - Requires that commercial email be identified as an advertisement and include the

sender's valid physical postal address.

b. Customer may not use EpiGrid services to:

●"Harvest" email addresses from Web sites or Web services that have published a notice prohibiting the transfer of email addresses for the purpose of sending email or participate in the use of software (including "spyware") designated to facilitate this activity.

●Generate email addresses using a "dictionary attack"—combining names, letters, or numbers in to multiple permutations.

●Use scripts or other automated ways to register for multiple emails or user accounts to send commercial email.

●Relay emails through a computer or network without permission—for example, by taking advantage of open relays or open proxies without authorization.

●Use another computer without authorization and send commercial email form or through it.

●Use a computer to relay or re-transmit multiple commercial email messages to deceive or mislead recipients or an Internet access service about the origin of the message.

●Falsify header information in multiple email messages and initiate the transmission of such messages.

●Register for multiple email accounts or domain names using information that falsifies the identity of the actual registrant.

●Falsely represent the sender as owners of multiple Internet Protocol addresses that are used to send commercial email messages.

iii. **<u>Vulnerability Testing</u>**.

Customer may not attempt to probe, scan, penetrate, or test the vulnerability of, or otherwise compromise the EpiGrid Equipment or Network or to breach EpiGrid's security or Customer Account authentication procedures without EpiGrid's prior written consent.

iv. **<u>IP Addresses</u>**.

EpiGrid will register Internet Protocol Addresses (IP Addresses) in Customer's name as part of the formation of the Customer's Account. EpiGrid will retain ownership of such data containing the IP addresses. If the IP addresses registered for the Customer are identified as contributing to the violation of this Policy, then the Customer will be in violation of this Policy, and EpiGrid may take reasonable action to protect the IP addresses, including suspension or termination of Customer's Account.

Further more, IP addresses must be maintained by Customer in an efficient manner as deemed by the American Registry of Internet Numbers (ARIN) and utilized at 80% within the later of i) thirty (30) days of registration by EpiGrid, or ii) fifteen days of delivery to Customer. Failure to comply with this Section may result in the revocation of IP Addresses by EpiGrid five (5) days after notice is provided to Customer.

v. **Awareness of Violation of this Policy.**
If Customer becomes aware of a violation of this Policy, Customer shall be expected to (a) immediately notify EpiGrid and (b) use commercially reasonable efforts to remedy such violation immediately, if under the Customer's control. Failure by the Customer to notify or take action shall be a violation of this Policy.

vi. **Reporting Abuses**.
Abuses of the Premises, Equipment, Network, Content, or Customer Account must be reported to EpiGrid in writing. EpiGrid prefers and provides: the email address support@EpiGrid.com for this purpose.