DISASTER RECOVERY PLAN

1. **Inventory hardware and software:** We maintain an up-to-date list of all security vendor's contact information, for quick access and resolution to any disaster that may arise in respect to our system, and its capabilities.

2. **Downtime tolerance:** We tolerate little to zero downtime. You pay for our product to work and to work well. Bitsy agrees to proactively acknowledge possible and current threats and complications to it's system and to quickly fix bugs and/or other complications that affect the integrity of our system, tools and support procedures. Communication in regards to downtime will occur at least once every 24 hours.

3. **Responsible personnel:** We maintain a regularly updated list of who is responsible for declaring a disaster, detailing a list of appropriate steps to quickly amend such disaster, how to get in touch with essential third-party vendors (if applicable) involved in resolution thereof and who is responsible for carrying out our succession plan.

4. **Communication Plan:** We are in continual communication with one another for day-to-day operations. We continue to maintain best points of contact for all parties involved in the successful operation of our business and the services provided to our customers.

5. **Where to go in case of emergency:** As all of our operations are currently mobile and remote, we encourage all employees to seek safe shelter first, that is familiar to that individual and would be considered reasonable to privately operate within and once established, get in touch with management to determine current position within all recovery plans.

6. **Service-Level Agreements (SLAs):** We maintain, in addition to our own, binding agreements with all contributors to our service that clearly defines levels of responsibility in the event of disaster.

7. **Sensitive Information:** Sensitive information of our member's clientele is primarily maintained by our members. Sensitive information of our member's is maintained by third-party vendors in nondescript facilities located in the United States of America. These critical facilities have extensive measures in place to ensure the security of housed information. Physical access is strictly controlled by authorized individuals under the employ of such third-party vendors. Authorized staff must pass required authentication procedures set forth by the employing entity. We do not share, by any means, personal information pertaining to our members and that of their clientele.

8. **Testing:** Regular testing ensures our plan will be effective in the event of disaster. We test our plans and procedures for recovery at least 2 – 4 times annually.