**Comprehensive Systems Control Plan**

**Introduction**

The purpose of this document is help ensure business continuity. The client will need to process transactions without interruption in the event of a threat. This document helps to ensure that threats have a mitigation plan.

**Data Entry Controls**

**Input Errors** can be a typo from a user inputting a change in inventory. For example, ‘11’ instead of ‘1’ for a quantity of bottles.

* Check to make sure all fields have a valid entry
* Validate that all fields have the correct format
* Validate that all fields are within the correct scope

To ensure valid entries are made into the system input masks will be used within Access.

**Audit Control** isimportant to ensure that information is accurate and backups are ran when necessary. Audit control will also help to ensure that information is current.

* Keep track of when orders are made and by whom
* Keep track of when backups are ran and by whom

To ensure audit control, logs will be implemented in Access to keep track of specific information.

**Output Controls-** the data in this system is not confidential so output controls will not be necessary.

**Database Controls** will include a backup to an external hard drive. This will help to ensure that in the event of a system crash, the system will be easy to restore.

* Database will be backed up every week on pc and external hard drive

**Access Controls** will include using a password to gain access to database. This will help to ensure that only people with proper credentials are using the system.

**Software Controls**

**Unintentional Errors**

* **Software bugs** will be avoided by updating Microsoft Access regularly and running Windows update to check for updates on weekly basis.

**Intentional Errors**

To avoid intentional errors, such as viruses and malware, an anti-virus will need to be installed. Team Awesome suggests using Symantec. This software will be scheduled to run weekly to keep up with scans and updates.

**Hardware Controls**

**PC Control** will begin with the PC remaining in the existing office, which is kept locked when no one is in there. The PC and external hard drive will utilize a surge protector. The external hard drive will be kept in the safe that is currently in office.

**Disaster Recovery Section**

**Contention Plan**

In case of a disaster the PC will be in a locked office, and the external hard drive will be in a locked safe. The safe should protect against most natural disasters that might occur in this region. If a disaster is predicted to happen, the system will be shut down and stored. The user will then use their contingency plan.

**Contingency Plan**

In the event of a disaster the client will resort to using their current method of pen and paper while the system is out.

**Recovery Plan**

In the event of a recovery, if the PC is not operable a new one will be purchased. When a working PC is established, the backup from the external hard drive will be mounted on the PC. The pen and paper transactions will then be input into the system so the data in the system is up to date.