Backup & Recovery Procedure

Prepared by: Justin McNaughton

Table of Contents

1. Introduction 1
2. Backup Strategy 2
3. Recovery Process 3
4. Security & Review Procedures 3

1. Introduction

The Mocha Point Inventory Management Application is a desktop-based system developed using C# and SQLite. It is designed for use by Mocha Point Management to handle tasks such as tracking ingredients, drinks, inventory levels, and alert notifications for low supplies. The application offers password-protected access for users. All data is stored in a single SQLite file named inventory.db. For new users, understanding how to protect and restore this data is important.

---

2. Backup Strategy

New users should focus on regularly backing up two main components: the application files and the database. These files are located in the Release folder, found under:
Desktop > folder > current app > inventory > Release.

The folder includes the application file (MochaPointInventory.exe), required .dll dependencies, and the inventory.db file which holds all critical data. Each week, users should compress this folder into a .zip file named using a date format such as MochaInventoryBackup_YYYY-MM-DD.zip and upload it to a secure cloud storage solution like Google Drive.

In addition to the weekly full-folder backup, it's recommended to make daily backups of the inventory.db file. This can be done by copying it manually to a secondary folder, or automated using scripts. Regular backups reduce the risk of data loss due to file corruption or accidental deletion.

.

---

3. Recovery Process

In the event of an application failure or data loss, restoring the system is straightforward. The user should begin by downloading the most recent .zip backup from Google. To run the application, simply open the MochaPointInventory.exe file.

If the inventory.db file requires restoration, the user can copy a previously saved version of the file into the application folder. Additionally, the application includes a Backup Database button within the interface, allowing users to create and manage backups directly from the app with no technical expertise being required. Once the necessary files are in place, test key features such as logging in, checking inventory, and viewing notifications to make sure the system is functioning correctly.

---

4. Security & Review Procedures

Protecting the backup files is important. All backups should be stored on a secure, access-controlled Google Drive account. The inventory.db file remains local and is never shared online, to reduce its vulnerability to cyber threats.

User authentication within the application is handled through the UserSettings table in the VS database. If incorrect credentials are entered, users are prompted to retry, which offers both usability and security.

To maintain system integrity, new users should participate in scheduled reviews of the backup and recovery process. This includes a quarterly review of procedures and a full test of application and database restoration every six months. Documenting results from these tests will help with accountability and continuous improvement.