FLOOD COMMERCE PLATFORM – ADMINISTRATOR GUIDE

Version 1.0 (Sample)
Prepared by: Lavanya S

1. Introduction

This Administrator Guide describes the configuration and maintenance tasks required to operate the Flood Commerce Platform. It is intended for IT administrators and implementation engineers who manage users, stores, access control, and integrations.

2. Administrator Responsibilities

Typical responsibilities of a Flood administrator include: - Creating and deactivating user accounts - Assigning roles and permissions - Adding new stores and channels - Managing API credentials and webhooks - Monitoring system health and troubleshooting

3. User Management

3.1 Creating Users

1. Sign in with an administrator account.
2. Navigate to Admin > Users.
3. Click Add User.
4. Enter Full Name, Email Address, optional Mobile Number, and Role (Viewer, Agent, or Admin).
5. Click Create User.

After creation, the user receives an activation email.

3.2 Disabling Users

1. In Admin > Users, search for the user.
2. Open the user record.
3. Set Status = Inactive and click Save.

Inactive users can no longer log in but their transaction history is preserved.

4. Store Management

4.1 Adding aStore

1. Navigate to Admin > Stores.
2. Click Add Store.
3. Enter Store Name, Store Code, Address, and Time Zone.

4. Select default currency.
5. Click Save.
The store becomes available to authorized users.

4.2 Assigning Users to Stores
1. Open Admin > Stores.
2. Select the desired store.
3. Go to the Users tab.
4. Click Assign Users.
5. Select user(s) and click Apply.

5. Role and Permission Model
Flood uses a role-based access control (RBAC) model. Users inherit permissions assigned through their roles.

5.1 DefaultRoles
Viewer – Read-only access to dashboards and reports.
Agent – Create and manage orders and customer records.
Admin – Full operational and configuration access including APIs and integrations.

6. API Credentials Management

6.1 CreatinganAPI Client
1. Navigate to Admin > API Clients.
2. Click New Client.
3. Enter a Client Name (e.g., POS Integration – Chennai).
4. Select scopes such as orders.read, orders.write, users.read.
5. Click Generate.
Flood issues a Client ID and Client Secret for system integrations.

6.2 RevokinganAPI Client
If credentials are compromised:
1. Locate the API client under Admin > API Clients.
2. Set Status = Revoked.
3. Click Save.
All API calls using revoked credentials return HTTP 401 Unauthorized.