# **User Authentication & Management Spec**

## **Perspective 1: User**

* **Signup**
  + Register with email + password.
  + Receive verification email (expires 24h).
  + Verified users get a unique user\_id (UUID).
* **Login**
  + Email + password check.
  + If banned → see restriction message, no session created.
* **Password Recovery**
  + Request reset link (expires 1h).
  + Submit new password → sessions invalidated.
* **Account Deletion**
  + Soft delete (status=deleted, recoverable for 30d).
  + Hard delete (permanent, requires confirmation).
* **Dashboard**
  + View profile: email, created\_at, last\_login.
  + Recent activities (logins, resets, changes).
  + Security (2FA status, active sessions).
  + Download/export personal data (JSON).

## **Perspective 2: Admin**

* **Dashboard (Private)**
  + Metrics: total users, active, banned, deleted.
  + Search users by user\_id or email.
* **User Controls**
  + Add user (optional, with email verify).
  + Ban / Unban (set reason, optional expiry).
  + Delete user (soft or hard).
  + Export user data.
* **Audit**
  + Every action logged (who, what, when, why).
  + Log retention ≥1y.

## **Data Model (simplified)**

1. ****User: {id, email, password\_hash, email\_verified, status[active|banned|deleted], created\_at, last\_login}
2. AuthToken: {id, user\_id, type[session|pw\_reset|verify], expires\_at}
3. ActivityLog: {id, user\_id, actor\_id, action, details, created\_at}



## **Endpoints (Core)**

* /api/auth/signup → register + email verify
* /api/auth/login → login / ban message
* /api/auth/password-reset/request + /confirm
* /api/user/delete → soft/hard delete
* /api/user/me/dashboard → user history
* /api/admin/stats → totals
* /api/admin/users?query= → search
* /api/admin/users/{id}/ban|unban|delete|export

## **Security Defaults**

* Password hashing: **Argon2id** (or bcrypt).
* Email tokens: random, single-use.
* Sessions: short-lived (15m) + refresh (7–30d).
* Rate limits: logins, signups, resets.
* Admin accounts: 2FA required.
* GDPR: export + right-to-delete supported.

## **Example Messages**

* **Signup**: “Check your email to verify your account.”
* **Login (banned)**: “Your account has been restricted. Contact support.”
* **Password Reset**: “If your email exists, you’ll receive a reset link.”
* **Delete**: “Data will be removed after 30 days. Type DELETE to confirm.”

✅ Fits on one page — easy to print or drop into Replit as a README/spec.

Do you want me to **format this directly into a Replit-ready Markdown file** (so you can copy-paste into README.md), or a **PDF export** that you can download?