Handz V1 PRD Bundle

CH07 — Authentication & Account System

Doc ID: HZ-V1-CH07_Authentication_Account_System_R1 • Revision: R1 (2026-01-02) • Status: Draft

Required Front-Matter (CH00 §2)

- **Doc ID:** HZ-V1-CH07_Authentication_Account_System_R1
- **Revision:** R1 (2026-01-02)
- **Status:** Draft
- **Depends on:** CH02 (Constraints), CH08 (Entitlements & Plan States), CH30 (Safety/Abuse), CH28 (Offline Behavior & Sync)
- **Related:** CH01 (V1 Scope), CH04 (Navigation Map), CH05 (Screen Inventory), CH25 (Monetization), CH31 (Error States), CH34 (Data Export & Account Deletion)
- **Supersedes:** None (first revision)
- **Owned Decisions:** Authentication methods (Apple/Google/Email), Guest behavior & restrictions, conversion prompts, session management, account UI copy for auth flows (non-marketing).
- **Open Questions / Placeholders:** None for provider set; numbers/limits are owned by CH08/CH25/CH30; any change requires updating those chapters and cross-referencing here.

1. Purpose and Scope

This chapter specifies **exactly how users create an account, sign in, stay signed in, and convert from Guest** in Handz V1. It defines required screens, UI copy, validation, routing, and gating rules tied to authentication. It does **not** define pricing, paywalls, or entitlement limits; those are owned by CH08/CH25 (see cross-references).

Primary outcomes for V1:

- A new user can start in seconds (Guest browse) and understand what Handz does without confusion.
- A motivated user can create an account with minimal friction (Apple/Google/Email).
- Guests are prevented from generating “free value loopholes” (no saving flows, no local saved drafts) while still experiencing meaningful demo value.
- All account-required actions trigger clear, consistent conversion prompts that feel fair and explain the value (not just “paywall”).
- Auth is reliable, secure, and App Store compliant on iOS (Apple sign-in offered when other providers exist).

2. Definitions

- **Guest:** A user who has not created an account. Guest sessions can browse demo content but cannot save user-created content. See CH08 §2 (Plan States).
- **Account User:** A user with an authenticated identity (Apple, Google, or Email).
- **Verified Email:** For Email sign-ups, a verified email address is required before access to account-required features is granted.
- **Conversion Prompt:** A modal or full-screen flow that encourages a Guest to create an account when they hit a gated action.
- **Session:** The authenticated runtime state: tokens stored securely, refresh handled automatically, and the user can close/reopen the app without re-auth (unless revoked).

3. Authentication Providers

Handz V1 supports three sign-in methods: **Sign in with Apple**, **Google**, and **Email**. All three methods must be available from the Welcome Gate, and from any conversion prompt that blocks progress.

3.1 Sign in with Apple (iOS primary)

- Apple sign-in button uses Apple Human Interface Guidelines styling (black or white, depending on theme).
- Requested scopes: email, full name (name is optional; do not block if name is unavailable).
- On first sign-in, capture Apple-provided email (may be private relay). Store it as the account email.
- If Apple returns no email on subsequent sign-ins, use the stored email; do not re-prompt.
- If the Apple credential is revoked, force logout and show a clear re-auth screen.

3.2 Google sign-in

- Google sign-in is offered as a convenience option for users who prefer it.
- Email address from Google becomes the primary email identifier (used for receipts, export notices, account recovery).
- If the Google email already exists in the system under Email auth, the user is logged into the existing account (account linking rules below).

3.3 Email sign-up and login

- Email sign-up requires: email + password.
- Email login requires: email + password.
- Email verification is required before account-required features unlock (see §6.4).
- Password reset is supported via “Forgot password” link on the login screen.

3.4 Account linking rules (provider collisions)

If the same email is used across providers, Handz must avoid accidental duplicate accounts. V1 rule: **merge-by-email** when safe; otherwise prompt the user.

- If Google sign-in email matches an existing Email-auth account, link Google to that account after successful Google auth.
- If Apple sign-in returns the same email as an existing account, link Apple to that account.
- If Apple uses private relay and the user later signs up with their real email, treat as a separate account (no automatic merge). Provide a manual support path later (out of scope V1).
- Never auto-merge accounts if it would overwrite an existing user profile without confirmation.

4. Account Profile Model (V1)

The account system defines the minimal profile fields required for sharing, attribution, and future community expansion. V1 keeps this minimal to reduce friction while keeping forward-compatibility.

- **User ID:** immutable UUID (internal).
- **Display Name:** optional at sign-up; can be set during onboarding. Used for attribution when sharing.
- **Handle:** optional in V1; recommended. If collected, must be unique (case-insensitive).
- **Avatar:** optional. Default is generated initials tile.
- **Created At:** timestamp.
- **Plan State:** Guest/Free/Pro/Trial (owned by CH08).

Handle rules (if enabled in V1):

- Allowed characters: a-z, 0-9, underscore. No spaces.
- Length: 3 to 20 characters.
- Case-insensitive uniqueness ("Handz" and "handz" are the same).
- Validation happens as user types (spinner then available/unavailable).
- If user skips handle, the system generates a temporary one (e.g., user-483921) and lets them set later in Settings.

5. Guest Mode (Try Without Account)

Guest mode exists to reduce friction because most users do not yet understand “flows.” However, Guests must not be able to bypass account creation and still obtain durable value.

5.1 Guest capabilities (allowed)

- Browse demo flows and demo move library (read-only).
- Open the Flow Detail View for demo flows (view-only).
- Enter a guided “What do you want to do?” onboarding chooser (learn/build/practice), but “build” routes to account creation before editing begins.

- View the Practice mode demo (predetermined session) if enabled by CH25 (demo-only).

5.2 Guest restrictions (hard blocks)

- **No saving flows:** Guests cannot save flows locally or remotely. Any attempt to create/save triggers conversion prompt. (Global lock in CH00 Decision Log.)
- **No saving custom moves:** Guests cannot create or persist custom moves. Move creation triggers conversion prompt.
- **No practice on user-created flows:** Practice is paywalled and also account-required; Guests can only access a demo practice experience, if enabled.
- **No inbox imports:** Guests cannot accept imported flows into an inbox. Shared links can be viewed in read-only mode.

5.3 Guest data handling

- Guest sessions may have ephemeral UI state (e.g., last viewed demo flow) stored locally for convenience, but it must be safe to delete at any time.
- Do not store any user-authored content for Guests (no drafts that could later be recovered).
- If a Guest begins building a flow (e.g., in a sandbox), the moment they attempt to add the first node, show an account gate **before** any meaningful work occurs.

6. Conversion Prompts (Account Required)

Conversion prompts are consistent, predictable, and explain the **why** in one sentence. They always offer Apple/Google/Email. They never feel like an error; they feel like a next step.

6.1 Global conversion prompt design

- Presented as a modal sheet (preferred) or full-screen if deep flow required.
- Always includes: title, one-sentence value, provider buttons, secondary action ("Not now" or "Continue browsing").
- If the user previously dismissed conversion, the second time includes an additional line: “Saving requires an account so your plans don’t get lost.”
- Never show “Try without account” inside conversion prompts (that would loop).

6.2 Conversion prompt triggers (V1)

- Tap: **Create New Flow** (first entry point to building).
- Attempt to add first node to a new flow canvas.
- Tap: **Save** or **Done** on any editable content.
- Tap: **Create Move** or **Save Move**.
- Tap: **Practice** on any non-demo flow.
- Tap: **Duplicate** a shared flow into Library.

- Tap: **Save from Inbox** (Inbox itself is account-only, but keep this rule for safety).

6.3 Conversion prompt copy (baseline, non-final marketing)

Use these strings verbatim unless CH15 updates them:

```
Title: Create an account to save
Body: Handz saves your flows and drills across devices. Guests can browse, but saving requires an account.
Buttons: Continue with Apple • Continue with Google • Continue with Email
Secondary: Not now (keeps browsing demo content)
```

6.4 Email verification gating

- After Email sign-up, user enters the app but is in a **limited** state until email is verified.
- Show a persistent banner: “Verify your email to protect your account.” with actions: [Resend] [I’ve verified].
- Account-required features remain accessible only if they do not risk account takeover; saving flows remains allowed but flagged until verification? **V1 rule:** saving flows is allowed immediately, but sharing and export require verification (safer).
- If you prefer stricter: block saving until verified. If that change is desired, create PLACEHOLDER in CH00 and decide later.

7. Session Management

The app must keep users signed in across launches, handle token refresh automatically, and provide a reliable logout.

7.1 Persistent login

- On successful auth, store session tokens securely (iOS Keychain).
- On app launch, attempt silent session restore. If valid, route user to the main app.
- If session expired, show a re-auth screen with last-used provider highlighted.

7.2 Logout

- Settings includes a Logout button.
- Logout clears session tokens and returns to Welcome Gate.
- Logout does not delete local cached content unless user chooses “Clear cache” (owned by CH28).

7.3 Multi-device behavior

- User can be logged in on multiple devices.
- Edits sync is owned by CH28; auth only guarantees identity.
- If user changes password (Email auth), other devices remain logged in until tokens expire, unless provider supports global sign-out.

8. Auth Screens and UI Specs

CH05 owns the authoritative screen inventory; this chapter defines the auth screens in detail and their behaviors. All routes must also exist in CH04 Navigation Map.

8.1 Welcome Gate

- **Route ID:** auth/welcome
- **Purpose:** First-run entry. Explain what Handz is and offer sign-in options. Allow Guest browse.
- **Components:** App logo, tagline, 3 provider buttons (Apple/Google/Email), “Log in” link, “Try without account” secondary button.
- **Primary actions:** Continue with Apple; Continue with Google; Continue with Email; Log in; Try without account.
- **Validation:** None.
- **Error states:** No internet: show inline banner “You’re offline. Sign-in requires internet.” Disable provider buttons; allow Guest browse if demo is cached.
- **Navigation:** If authenticated session exists: skip to main app. If Guest taps Try: route to demo dashboard (home/demo).

8.2 Choose Email Path (Sign up vs Log in)

- **Route ID:** auth/email_choice
- **Purpose:** Avoid confusion for email users by explicitly choosing sign-up or login.
- **Components:** Two large buttons: “Create account with email” and “Log in with email”.
- **Primary actions:** Choose one path.
- **Validation:** None.
- **Error states:** None.
- **Navigation:** Back returns to Welcome Gate. Continue routes to auth/email_signup or auth/email_login.

8.3 Email Sign-Up

- **Route ID:** auth/email_signup
- **Purpose:** Create a new account using email + password.
- **Components:** Email input, password input, password strength hint, Terms/Privacy links, primary button “Create account”, link “Already have an account? Log in”.
- **Primary actions:** Create account.
- **Validation:** Email format; password minimum 8 characters; disallow common passwords (basic blacklist).
- **Error states:** Email already used → “This email is already in use. Log in instead.”; weak password; network failure.
- **Navigation:** Success routes to onboarding/profile_setup with “verification banner active”.

8.4 Email Log-In

- **Route ID:** auth/email_login
- **Purpose:** Login to existing account using email + password.
- **Components:** Email input, password input, “Forgot password?”, primary “Log in”.
- **Primary actions:** Log in; Forgot password.
- **Validation:** Email format; password non-empty.
- **Error states:** Wrong credentials → “Incorrect email or password.”; account disabled; network failure.
- **Navigation:** Success routes to main app home. Forgot password routes to auth/forgot_password.

8.5 Forgot Password

- **Route ID:** auth/forgot_password
- **Purpose:** Send a password reset email.
- **Components:** Email input, button “Send reset link”.
- **Primary actions:** Send reset link.
- **Validation:** Email format.

- **Error states:** Email not found → “No account found for that email.”; network failure.
- **Navigation:** After success show confirmation screen and option back to login.

8.6 Profile Setup (Optional)

- **Route ID:** onboarding/profile_setup
- **Purpose:** Collect display name and optional handle/avatar; keep minimal.
- **Components:** Display name input, handle input (optional), avatar picker (optional), “Continue” button, “Skip”.
- **Primary actions:** Continue; Skip.
- **Validation:** If handle entered: validate allowed chars and uniqueness.
- **Error states:** Handle taken; invalid chars; network failure.
- **Navigation:** Continue routes to onboarding/goals_router. Skip routes to onboarding/goals_router.

8.7 Goals Router (Onboarding chooser)

- **Route ID:** onboarding/goals_router
- **Purpose:** Ask what user wants to do first and route accordingly.
- **Components:** Question cards: “Build a gameplan”, “Practice a gameplan”, “Browse examples”.
- **Primary actions:** Select an option.
- **Validation:** None.
- **Error states:** None.
- **Navigation:** Build routes to flow/create (account required - already satisfied). Practice routes to practice/setup (may be paywalled; see CH25). Browse routes to library/demo.

8.8 Guest Browse Dashboard

- **Route ID:** home/demo
- **Purpose:** Guest-only home that makes value clear and drives conversion.
- **Components:** Demo flow cards, “What is a flow?” explainer card, CTA “Create an account to build yours”.
- **Primary actions:** Open demo flow; Watch demo practice; Create account.
- **Validation:** None.
- **Error states:** None.
- **Navigation:** Opening demo flow routes to flow/detail_demo (view-only). Create account routes to auth/welcome.

9. Gating Rules Owned by CH07

These rules are specifically owned here because they describe **authentication gating**. Limits and paywalls are owned by CH08/CH25/CH30.

- **Rule CH07-G1:** Guests cannot enter the editable flow builder. Tapping any build entry point triggers the conversion prompt first.
- **Rule CH07-G2:** Guests cannot save flows locally or remotely. There is no “draft recovery” for Guests.
- **Rule CH07-G3:** Guests cannot create or persist custom moves. Attempting move creation triggers conversion prompt.
- **Rule CH07-G4:** Shared links opened by Guests are view-only. Any attempt to duplicate/save triggers conversion prompt (and then proceeds after signup).
- **Rule CH07-G5:** After signup from a conversion prompt, return user to the exact pre-gate context (e.g., the flow they were trying to duplicate).

10. Security, Privacy, and Compliance Notes

- Store auth tokens securely (iOS Keychain). Do not store plain tokens in AsyncStorage.
- Use HTTPS for all network calls; reject insecure endpoints.
- Throttle login attempts to reduce brute force (see CH30 for escalation messaging).
- Do not expose whether an email exists in the system in a way that enables account enumeration beyond standard UX (balance with helpfulness).
- Provide Terms and Privacy links on account creation screens.
- Support “Restore Purchases” in Settings (owned by CH25) but auth must not block restore flows.

11. Acceptance Tests (Given/When/Then)

- **AT-07-01** Given I am logged out, when I open the app, then I see Welcome Gate with Apple/Google/Email and Try without account.
- **AT-07-02** Given I am a Guest, when I tap Create New Flow, then I see the conversion prompt and cannot reach an editable canvas without creating an account.
- **AT-07-03** Given I sign up with Email, when I enter a weak password, then the Create account button is disabled and I see “Password must be at least 8 characters.”
- **AT-07-04** Given I sign up with Email, when I complete signup, then I enter the app and see a verification banner until verified.
- **AT-07-05** Given I sign in with Apple, when auth succeeds, then I land in the main app and the session persists across app relaunch.
- **AT-07-06** Given I fail login 5 times, when I attempt again, then I see a throttling message and must wait before retrying (thresholds owned by CH30).

- **AT-07-07** Given I am a Guest viewing a shared link, when I tap Duplicate, then I am prompted to create an account and after signup I return to the duplicate flow flow.
- **AT-07-08** Given I log out, when I reopen the app, then I return to Welcome Gate and cannot access authenticated screens via back navigation.

Acceptance Checklist

- All provider buttons work on a real iOS device (not just simulator).
- Guest cannot enter editable builder or save any user-authored content.
- Conversion prompt appears on every gated action listed in §6.2.
- Email auth supports signup, login, forgot password, and verification banner.
- Logout reliably clears session and blocks back navigation to private screens.
- All error states display readable copy (no raw exceptions).

12. Replit Build Prompt (CH07 only)

```
You are implementing Handz V1 PRD Bundle: Chapter CH07 Authentication & Account
System only.
Bundle ID: HZ-V1. Follow CH00 rules: no guessing, cross-reference dependencies, and
stop if an assumption is needed.

Implement the following, in order:
1) Routing: Create route IDs exactly as listed in CH07 §8 (auth/welcome,
auth/email_choice, auth/email_signup, auth/email_login, auth/forgot_password,
onboarding/profile_setup, onboarding/goals_router, home/demo).
2) Welcome Gate UI: 3 provider buttons + Try without account. If offline, disable
provider buttons and show banner. If session exists, auto-navigate to main app.
3) Provider auth: Sign in with Apple (iOS), Google sign-in, and Email sign-up/login
flows. Store session tokens securely (Keychain).
4) Guest rules: Enforce CH07-G1..G5. Guests must not access editable flow builder or
save flows/moves locally. Any attempt triggers conversion prompt modal.
5) Conversion prompt: Build a reusable modal component with title/body/buttons per
CH07 §6.3. Ensure post-signup returns user to pre-gate context.
6) Email verification banner: After Email sign-up, show persistent banner with Resend
and I've verified; block sharing/export until verified (note: saving flows allowed).
7) Logout: Add Settings action that clears tokens and resets navigation stack to
Welcome Gate.

Do NOT implement monetization screens, practice gating, flow builder, or storage
limits beyond the Guest gates described here.
If you need CH08 or CH25 details (plan state detection, paywalls), stub them behind a
feature flag and write a "PRD Assumptions" comment block listing what you need.
```

13. Troubleshooting Notes (CH07)

- **Apple sign-in works on simulator but fails on device:** verify bundle ID, entitlements, and Apple sign-in capability enabled.
- **Google sign-in redirect errors:** confirm OAuth client IDs for iOS and correct redirect URI scheme.
- **Email verification never clears:** ensure verification status is re-fetched from auth provider after "I've verified" tap.
- **Users can access private screen after logout via back button:** reset navigation stack; do not just navigate.
- **Conversion prompt loops:** ensure "Not now" only returns to browsing demo routes, never to gated build routes.
- **Duplicate accounts created:** confirm merge-by-email logic in §3.4 and prevent auto-merge on private relay emails.