Handz V1 PRD Bundle

CH30 — Safety/Abuse Limits & Warning Ladder (R1)

Generated: 2026-01-02 • Bundle ID: HZ-V1

Required Chapter Header Block (CH00 §2)
Doc ID: HZ-V1-CH30_Safety_Abuse_Limits_Warning_Ladder_R1
Revision: R1 (2026-01-02)
Status: Draft
Depends on: CH00, CH08, CH17, CH18, CH20–CH22, CH29, CH31
Related: CH25, CH27, CH33, CH34
Supersedes: (none)
Owned Decisions: safety ladder levels L0–L5; soft-cap philosophy; enforcement surfaces & UX copy rules; safety-owned limits & escalation mapping
Open Questions / Placeholders: share-link caps + thresholds; cooldown durations; edit/import rate thresholds; admin tooling scope

Chapter Index

1. Purpose & Scope

This chapter defines the complete, V1-shippable safety and anti-abuse system for Handz. It covers: (a) what constitutes abuse; (b) the user-visible warning ladder; (c) the plan-aware caps and soft caps; (d) enforcement behavior across Guest/Free/Pro/Trial; (e) recovery and support paths; and (f) the minimum viable detection and logging needed to keep the system safe without making legitimate fighters/coaches feel restricted.

Non-goals: community moderation, public content moderation, harassment reporting, and gym/community roles are out of V1. This is strictly about protecting app resources, preventing spam/automation, avoiding accidental data-loss, and preserving user trust when limits apply.

2. Threat Model

We protect against:

- Resource abuse: automated or excessive creation of share links, imports, flows, or edits that stresses backend and harms service quality.
- Spam distribution: mass generation of unlisted share links to distribute unwanted content (even if unlisted).
- Storage abuse: attempts to exceed media/storage caps (especially video) or repeatedly upload/delete to probe limits.
- Account farming: many guest sessions or many new accounts from one device/network used to bypass caps.
- Denial of service vectors: repeated heavy operations (e.g., exporting, importing, opening huge flows) to degrade app.
- User self-harm via UX: confusing caps that cause people to lose work or feel trapped; punishing messages that cause churn.

We explicitly do not protect against (V1):

- Public feed toxicity or open posting (no public feed in V1).
- DM harassment (no DMs in V1).
- Copyright enforcement on user-linked videos (links are user-provided).

3. Definitions & Global Principles

3.1 Key terms

Term	Meaning
Cap	A hard stop that prevents an action (e.g., “You cannot save more flows”).
Soft cap	A threshold where we warn and/or slow the user down, but still allow progress; repeated exceedance can escalate.

Warning ladder	A progressive escalation system L0–L5 that communicates risk/limits and applies proportionate enforcement.
Enforcement action	Any automatic measure: UI warning, cooldown, temporary block, or account restriction.
Recovery	How a user returns to normal: wait for cooldown, upgrade plan, or contact support.

3.2 Global principles (non-negotiable)

- **Soft caps by default**: Limits should feel like guardrails, not punishments. We warn early and only block when necessary.
- **No silent failure**: When an action is blocked or degraded, we must show why, what to do next, and how to recover.
- **Don’t destroy work**: If a user hits a cap, the app should preserve drafts and offer clear choices (upgrade, delete, export, later).
- **Plan-aware but respectful**: Free users should feel usable (explore/build basics), and Pro should feel smooth—not unlimited.
- **Cross-reference ownership**: If a rule is owned by another chapter, reference it using CH00’s format; do not redefine it here.
- **Reversible states**: Provide a “revert” path when a safety action changes user state (e.g., link revoked).
- **Transparent counting**: Show users what is counted toward a cap and what is not.

3.3 Locked limits & rules referenced (not owned here)

The following are V1 decisions referenced by CH30 for enforcement and messaging. Ownership stays with the listed chapter(s).

- See: HZ-V1-CH02 (Platform constraints: iOS-only, portrait-only).
- See: HZ-V1-CH07 (Auth options: Apple/Google/Email; Guest conversion).
- See: HZ-V1-CH08 (Plan states: Guest/Free/Pro/Trial; gating model).
- See: HZ-V1-CH15 (Saved flows cap for Free = 2).
- See: HZ-V1-CH18 (Inbox cap for Free = 10; Free inbox items are view-only).
- See: HZ-V1-CH20–CH22 (Practice paywall; Free gets 3 monthly practice credits; credits apply only to saved flows).
- See: HZ-V1-CH12 (Branch cap: 10 outgoing branches per move).
- See: HZ-V1-CH29 (Uploads: Pro only; 2GB total cap; uploads are private-only and not shareable).
- See: HZ-V1-CH25 (Pricing direction: $9.99/month; 7-day trial).

4. Warning Ladder (L0–L5)

The ladder describes **what the user experiences** and **what enforcement occurs**. Most actions begin at L0 (normal) and escalate when the same vector is abused or when signals suggest automation.

L0 — Normal

No warnings. User actions proceed normally. Light background counting may occur.

- No user-visible messaging.
- No throttling beyond standard API rate limiting.
- All counters tracked for potential escalation.

L1 — Informational Nudge

Early, friendly notice that they're approaching a soft cap.

- Non-blocking toast or inline banner.
- Provides: current usage + cap + how it resets.
- No slowdown; user can continue.

L2 — Soft Warning + Friction

User crosses a soft cap or repeats a risky action quickly; we add small friction.

- Inline warning card + optional cooldown (seconds/minutes).
- Optional confirmation step for repetitive actions (e.g., 'Create link').
- Still allows completion for legitimate users.

L3 — Temporary Cooldown / Partial Block

Clear misuse pattern or rapid repetition. Protect system with time-based restrictions.

- Action is blocked for a time window (e.g., 15–60 minutes) OR reduced (e.g., 1 link/hour).
- User sees countdown + reason + recovery options.
- Other parts of app remain usable.

L4 — Feature Suspension

Severe or repeated abuse. Suspend the feature category.

- Suspend share-link creation or media upload for 24–72 hours.
- User can still view their own content.
- Clear message + link to support + review steps.

L5 — Account Security Block

High-confidence automation/fraud signals or repeated L4; protect platform.

- Block high-risk actions (and possibly login) until verification/support.
- Show security screen with next steps.
- Audit log entry is mandatory.

4.1 Ladder escalation rules (generic)

- Escalation is per-vector (e.g., share-link creation vs media upload vs imports). A user can be L3 for links but L0 elsewhere.
- De-escalation happens automatically after cooldown windows unless signals persist. Do not permanently ‘brand’ users in V1.
- Escalation requires at least one of: (a) rate threshold exceeded; (b) repeated failures to comply (dismiss warnings + continue); (c) suspicious signal (see §6.2).
- Always log: vector, level, timestamp, device/session identifier, action counts, and user plan state (Guest/Free/Pro/Trial).

5. Limit Catalog & Escalation Mapping

This catalog lists each abuse-sensitive feature, the default plan-aware caps, the soft-cap triggers, and how ladder levels apply. Some exact numbers remain placeholders and must be finalized in the owner chapters; when numbers are placeholders, this chapter defines the **behavior** and the **kind** of limit.

5.1 Core limits (owned elsewhere; enforced here)

Vector / Feature	Guest	Free	Pro/Trial	See (Owner)
Save flows to library	Blocked	Max 2 saved flows	Higher/uncapped (placeholder)	CH07, CH08, CH15
Inbox capacity	N/A	Max 10 inbox items	Higher/uncapped (placeholder)	CH18
Practice sessions	Blocked	3 monthly credits on saved flows only	Unlimited (fair-use)	CH20–CH22, CH25
Outgoing branches per move	N/A	Max 10	Max 10 (V1)	CH12
Video uploads	Blocked	Blocked	Allowed; 2GB total cap	CH29

5.2 Abuse-sensitive vectors (owned by CH30)

These vectors are managed by CH30’s ladder. Exact thresholds may be tuned, but the behaviors below are locked.

Vector	**Abuse risk**	**Ladder behavior**	**Plan notes**
Share-link creation (unlisted links)	Users repeatedly generate many links in short time. Risk: spam distribution & backend load.	L1: approaching daily cap. L2: confirmation + short cooldown. L3: temporary block with countdown. L4: 24–72h suspension. L5: security block if signals persist.	Free cap + Pro cap are placeholders; owned by CH17/CH25 for pricing posture, but enforced via CH30 ladder.
Import acceptance (inbox receives)	Mass acceptance/import can be used to bypass flow limits or load the app with huge content.	Free: inbox cap 10 prevents infinite intake; saving limited by 2-flow cap. Burst imports trigger L2 confirm + small cooldown; L3 if continued.	Keep sharing funnel alive: receiving is easy; saving/practicing applies entitlements (CH18, CH15, CH20–CH22).
High-frequency edits (flow node spam, rename spam)	Automated scripts may spam edits to stress backend.	Server rate-limit; show L2 when user hits it; L3 cooldown if continued. Do not block normal 2-hour build sessions.	Thresholds are placeholders; final tuning belongs to CH12/CH13 owner + CH30 enforcement.

Video upload churn (Pro)	Upload/delete cycling to probe storage or create load.	L1 at ~80% storage. L2 at ~95% storage. L3 cooldown on repeated failed attempts. L4 upload suspension if repeated.	Storage cap is owned by CH29; ladder behavior is owned here.

5.3 Required UX behaviors at caps (locked behaviors)

- **Free hits saved-flow cap (2)**: allow viewing/editing existing saved flows. Block saving any additional flows. If user tries to save/import-to-library: show blocking modal with options: Upgrade to Pro, Delete a saved flow, Cancel (plus Export/Copy if CH34 supports it).
- **Free tries to practice**: if they have credits remaining and the flow is saved, allow. If credits are 0: show paywall (CH25). If flow is from inbox (not saved): block and explain 'Practice requires a saved flow' + CTA to save (may hit cap).
- **Free inbox is full (10)**: receiving new imports triggers an 'Inbox full' screen. Provide: Delete inbox items, Save one to library (if under cap), Upgrade to Pro.
- **Guest tries to save anything**: show conversion wall with Apple/Google/Email options (CH07) and a Cancel option.
- **Pro approaches 2GB storage**: show storage meter on upload UI; L1 banner at ~80%; hard block at 100% with actions: delete uploads or use links.

6. Implementation Rules

6.1 Single source of truth for limits

All caps and thresholds must be defined in a single configuration object (server-delivered if possible). Client reads the config to render counters and messaging. Server enforces the same config to prevent bypass. If server config cannot be delivered in V1, embed as constants but keep them centralized.

Required config fields (V1)

- planStates: guest/free/pro/trial
- caps: savedFlowsFree=2; inboxFree=10; practiceCreditsFreeMonthly=3; storageProBytes=2GB
- ladder: per-vector thresholds; cooldown durations; suspension durations
- copyKeys: mapping from vector+level → copy template keys
- resets: monthly credit reset; daily link reset; rolling-window counts (if used)

6.2 Suspicious-activity signals (V1 minimal)

- Very high rate actions (e.g., dozens of link creations in minutes) beyond plausible human use.
- Repeated failed attempts to perform blocked actions (e.g., spam tapping 'Create link' while in cooldown).
- Many new accounts from the same device/session identifier in a short window (account farming).
- High-frequency import acceptance with immediate delete cycles (churn).
- Unusually large flows or repeated attempts to create extremely large graphs (if graph size caps exist).

Important: treat signals as **probabilistic**. In V1 we prefer cooldowns over permanent bans. Avoid false positives that punish real coaches building big gameplans.

6.3 Placeholder thresholds (must be decided later)

- Exact share-link creation caps (Free/Pro) and rolling-window rate limits (owned by CH17/CH25; enforced by CH30).
- Edit-rate limit thresholds (per minute) that still allow 2-hour build sessions (owned by CH12/CH13; enforced by CH30).
- Import burst thresholds that catch automation without blocking normal coach sharing (owned by CH18; enforced by CH30).
- Cooldown durations per ladder level (e.g., L3 15–60 min; L4 24–72h).
- Storage warning thresholds for L1/L2 (recommended 80%/95%).

6.4 Telemetry requirements (minimum)

- Event: limit_counter_incremented (vector, plan, count, window)
- Event: ladder_level_shown (vector, level, plan)
- Event: action_blocked (vector, reason, plan, level)
- Event: cooldown_started / cooldown_ended
- Event: upgrade_cta_clicked (from which limit screen)
- Event: user_deleted_item_to_resolve_limit (flow/inbox/media)

7. UX Copy Rules & Templates

Copy must be: short, respectful, and actionable. Avoid shaming language. Always include a way forward.

7.1 Mandatory copy components

- **What happened**: ‘You’ve reached your Free plan limit for saved flows.’
- **Why** (1 sentence max): ‘This keeps Handz fast and prevents spam.’
- **What you can do next**: ‘Delete one flow, upgrade, or come back later.’
- **How counting works**: show the count and limit: ‘2 of 2 saved.’
- **Reset info** (when applicable): ‘Credits refresh monthly.’ ‘Link limits reset daily.’

7.2 Reusable templates (fill-in variables)

Template	Copy
Approaching soft cap (L1)	Heads up — you’re close to the limit for **{THING}** (**{COUNT}** of **{LIMIT}**).
Soft warning (L2)	You’re doing this a lot quickly. To keep Handz fast, we’ll add a short cooldown (**{COOLDOWN}**).
Cooldown (L3)	Temporarily paused: **{THING}**. Try again in **{TIME_REMAINING}**.
Feature suspension (L4)	**{THING}** is suspended for **{DURATION}** due to unusual activity. If this is a mistake, contact support.
Guest save wall	Create an account to save your work. It takes under a minute.
Practice paywall (credits 0)	Practice is a Pro feature. You’ve used your monthly credits. Start a 7■day free trial to keep drilling.
Inbox full (Free)	Your inbox is full (**{COUNT}** of **{LIMIT}**). Delete items or save one to your library.

7.3 UX surfaces (where messaging appears)

- Toast: L1 informational (non-blocking).
- Inline banner on the relevant screen (e.g., Practice setup, Share sheet): L1–L2.
- Blocking modal: when an action cannot proceed (cap reached) — must include next actions.
- Dedicated ‘Limit’ screen: for L3–L5, with countdown and support link.
- Settings > Plan: shows current counters and reset dates (recommended; see CH25/CH08).

8. Accessibility & Fairness

- Do not rely on color alone to communicate severity (use icons + text).
- Cooldown timers must be readable by screen readers and support dynamic type.
- Glove-on users: do not show non-critical safety prompts mid-practice timer; queue them for session end.
- Allow dismissal for L1/L2 banners, but keep a path to re-open details (e.g., ‘View limits’).
- Explain plan gating without shaming: ‘Free plan includes 2 saved flows’ instead of ‘You’re not allowed.’

9. Acceptance Tests

9.1 Given/When/Then (must pass to ship CH30)

1. Given a Guest user, when they attempt to save a flow draft, then the app blocks save and shows the Guest Save Wall with Apple/Google/Email options and a Cancel option.
2. Given a Free user with 2 saved flows, when they try to save a 3rd flow, then a blocking modal appears showing ‘2 of 2 saved’ and offers Upgrade / Delete Flow / Cancel.
3. Given a Free user with 0 practice credits remaining, when they start practice on a saved flow, then the app shows the Practice Paywall with trial info and does not start the timer.
4. Given a Free user, when they attempt to start practice from an inbox item, then the app blocks and explains that practice requires a saved flow, offering Save to Library (if possible) or Upgrade.
5. Given a Free user with 10 inbox items, when a new import arrives, then the app does not add it and shows Inbox Full screen with options to delete items or upgrade.
6. Given a Pro user at 85% of 2GB upload cap, when they open the upload UI, then an L1 banner appears and a storage meter shows current usage.
7. Given a user who creates share links rapidly beyond the L2 threshold, when they tap ‘Create link’ again, then the app shows L2 friction (confirmation + cooldown) and logs ladder_level_shown.
8. Given the same user continues beyond the L3 threshold, then link creation is blocked with a countdown timer and recovery steps.
9. Given a user exits cooldown window, when they retry the action, then normal behavior resumes (L0) unless suspicious signals persist.

9.2 Acceptance Test Checklist

- All locked caps (2 saved flows free, 10 inbox free, 3 monthly credits free, 2GB uploads pro-only) are enforced consistently in client and server.
- Ladder messages use templates and include count/limit and reset timing where applicable.
- No action silently fails; blocked actions always show a path forward (upgrade/delete/cancel).
- Cooldown timers update correctly and are accessible.
- All ladder events are logged with vector + level + plan state.
- Deleting flows/inbox items immediately updates counters and unblocks actions without app restart.
- Draft preservation: hitting caps never deletes a user’s draft without confirmation.

10. Replit Build Prompt + Troubleshooting

10.1 Replit build prompt (copy/paste)

```
You are continuing the Handz V1 PRD Bundle (Bundle ID: HZ-V1). You have CH00 and CH30.
Implement CH30 only; treat other chapters as dependencies (do not invent missing
rules).

Implement:
A) LimitsConfig: guest/free/pro/trial + locked caps:
- savedFlowsFree=2
- inboxFree=10
- practiceCreditsFreeMonthly=3 (usable ONLY on saved flows; never on inbox items)
- storageProBytes=2GB (uploads Pro-only; uploads are private-only and not shareable)
B) LadderManager (per-vector L0–L5):
- vectors: share_links, imports, uploads, edits
- inputs: plan, counters, suspicious signals
- outputs: ladder level, enforcement action, copy key
- store cooldown end timestamps; per-vector escalation only
C) Wire into actions:
- Save flow (guest blocked; free cap; pro ok)
- Start practice (credits + source type check)
- Receive import (inbox cap)
- Create share link (ladder-managed)
- Upload video (pro storage cap + ladder)
D) UI surfaces:
- L1 toast, L1–L2 inline banner, blocking modal for caps, dedicated cooldown screen for
L3–L5
- Must show: what happened + count/limit + next steps + reset timing (if any)
E) Telemetry:
- ladder_level_shown, action_blocked, cooldown_started/ended, upgrade_cta_clicked
F) Tests:
- unit tests for LadderManager
- integration tests for each action above (match Given/When/Then in CH30 §9.1)

If any threshold numbers (share link caps, cooldown durations, edit/import rate
limits) are missing, create PRD_ASSUMPTIONS.md listing them and stop the related
feature behind a TODO, rather than guessing.
```

10.2 Troubleshooting notes (common failures)

- **Counts don’t update after delete**: counters must derive from source-of-truth queries and re-render after mutations; do not cache stale counts.
- **Cooldown screen loops**: store cooldown end time once; compare with server time if available; ensure timer ends and state resets to L0 for that vector.
- **Free user can practice inbox item**: check source type (saved vs inbox) before credits check; inbox practice must always be blocked for Free.
- **Guest can save locally**: drafts may exist, but ‘Save to library’ must always route to Guest Save Wall and must not create a saved-flow record.
- **Storage cap inconsistent**: compute storage from server-tracked bytes; show meter; block uploads above remaining bytes; handle partial uploads safely.
- **False positives for power users**: tune edit/import thresholds; avoid escalating to L4/L5 in V1 without strong signals.