FreeholdIP

Issuing a Power of Attorney on FreeholdIP

You issue a secure, revocable digital record of a Power of Attorney your client owns — one that anyone can confirm is genuine and currently in force, without calling your office.

What this is — honestly

The record the executed instrument — it doesn’t replace it, or any execution formality under your state’s law. Its job is to let anyone confirm, without calling you, that a mandate is genuine and currently in force. Set client expectations accordingly:

- It’s strongest where no settled acceptance process exists — , where there is no clerk and RUFADAA visibly fails.
- With a traditional institution it *supports* the paper — most usefully as the “has this been revoked?” check — rather than supplanting the institution’s own process.
- It is also, simply, an authoritative of every mandate your firm has issued and its current status.

One-time setup

Your firm is a verified issuer with a signing/login file. Safeguard it like a signature stamp — it signs every mandate as your firm, and we never hold a copy. (Optional: bind your firm’s domain so your own domain vouches for your key.)

For each mandate

1. at `authority.freeholdip.com` with your firm’s login file — you land directly in the mandate console.
2. Connect it first and — the client’s name and address pre-fill from your own records, no re-keying. (Connect *before* unlocking your signing key: connecting hops to Clio and back, and the unlocked key lives only while the page stays open. The connection is per-session; we never store your Clio tokens or client data.)

3. — the key decrypts and signs in this browser only; we never see it.
4. send the client an (they fill in their own details and create their identity; it arrives back as a draft you review), or use the “✉ Invite” button beside each name. Creating an identity takes about two minutes.
   — your standard fiduciary safekeeping, and the client’s backstop if their own copy is lost.
5. — scope, effective (immediate or springing on incapacity), jurisdiction, limitations. Upload the executed Power of Attorney; its fingerprint is sealed into the record.
   — leave it unset and the mandate is in force until revoked, and the record says so plainly.
   Optionally name , with an exercise rule — acting singly, jointly, or by an M-of-N threshold. (See “Beyond the basic mandate,” below.)
6. — the mandate is signed in your browser with your firm key; we never see it.
7. the verify link, QR code, and downloadable copy to the client and the agent.
   One click files the *self-verifying copy* into the matter’s Documents — the firm’s system of record holds the artifact that keeps verifying even offline.
8. — revoke, reinstate, renew, or re-scope anytime under Manage; activate a named successor when the moment comes. Changes take effect immediately for anyone who checks.

Beyond the basic mandate

The same record carries authority through its whole life — the handoff on incapacity or death, and the self-custodied digital assets a custodian can never be served for. Each of these rides the same signed, revocable rail; none of it ever holds a key or an asset.

Multi-party roles & clean transitions

- Name co-agents who serve alongside the primary and ordered standby successors, with an exercise rule (single, joint, or M-of-N). The certification shows exactly who holds authority.
- When the triggering event occurs, you activate the named successor from Manage with your firm key. The certification then leads with *who is acting now*, on a clean, Bitcoin-anchored history — your defensible answer to “who held this authority, and when did it change?”
- Gate an incapacity transition behind typed two-physician attestations, a waiting period, and a protector’s veto — so it springs only when it should.

- Pre-authorize, at issuance, named attestors whose independent statements can activate a successor *even if your firm can no longer act* — checked by math at verify-time, with no call to the firm. A true continuity backstop for your clients.

Digital & self-custodied assets — the operate layer

- Issue a companion record that triages a client's assets: what a custodian can be compelled to disclose, versus the control-based assets the statute can't reach. It records references only (an xpub, a descriptor, a domain, a handle) — a fail-closed guard blocks anything that looks like a secret.
- For a control-based asset, attach a successor-only "how to take control" map — a Shamir-share plan, or a policy where the successor is a co-signer from the start. It is encrypted to the successor's own key before it reaches us; The shares and co-signing keys stay with the client's chosen people, and the successor reconstitutes control on the asset's own chain, on their own device. No key, share, or signature ever passes through you or us.

> **The non-custody line.** Everything above proves and coordinates a handoff; it never *performs* custody. That boundary is deliberate — keep client secrets in client/fiduciary custody, exactly as you would on paper.

Your responsibilities

- The accuracy of the mandate is yours, the same as any attestation you make.
- or its execution formalities.
- Neither you nor FreeholdIP ever holds the client's assets or keys. The record proves *who is authorized*; it never moves anything itself.
- For an inventory or a reconstruction recipe, you record where things are and who holds them — never a key or a share. The accuracy of that map is yours; the secrets stay in client/fiduciary custody.

An internet you own instead of rent. FreeholdIP — own your identity.