

Client Portal and Vaultwarden

Decision paper and implementation standard for client onboarding

Decision requested

Approve a three-system model: GoHighLevel for relationship and workflow data; Vaultwarden for credentials only; and a dedicated secure document portal/repository for client file uploads. Do not use either GHL or Vaultwarden as the universal repository.

Why this is the recommended design

- It gives every item one authoritative home, avoiding duplicate uploads and conflicting versions.
- It keeps passwords and account recovery details out of the CRM, while keeping CRM activity and onboarding workflow out of the password vault.
- It provides clients a normal file-upload experience for bank statements and identity records instead of asking them to use a password manager as a document portal.
- It makes offboarding, retention, access review, and incident response manageable by data type.

Scope and security boundary

This paper is an operating recommendation, not legal or compliance advice. Banking records, identity documents and credentials should be processed only after Blueprint confirms the applicable privacy, retention and professional-advice requirements for the engagement and jurisdictions involved. Never request or store one-time passcodes, card PINs, security-question answers, or client banking credentials unless access is explicitly necessary and authorized.

Decision matrix

Option	Benefits	Material limitations	Decision
Put everything in GHL	One familiar operational record; workflow and communications are native.	Credentials and high-risk financial/identity documents do not belong in CRM files. It creates excessive exposure for general CRM users.	Do not adopt.
Put everything in Vaultwarden	Encrypted vault items; suitable for sharing authorized logins and secure notes.	Not designed as a client-facing document-request, upload, versioning, checklist or status portal. Self-hosted operation adds backup and access-governance responsibility.	Do not adopt.
GHL + Vaultwarden only	Avoids a third system.	Forces sensitive documents into a tool that is not a document portal, or into the CRM. Poor client experience and muddied lifecycle controls.	Not recommended.
Three-system model	Clear purpose, least-privilege access, no duplication, client-friendly uploads and clean hand-offs.	Requires selecting and operating a secure document portal/repository.	Recommended.

The recommended operating model

Each system is authoritative for only the records in its lane. GHL references progress and links; it does not mirror document contents or secrets.

System	Primary job	Store here	Do not store here
GoHighLevel	CRM, sales/onboarding workflow and service communication.	Contact data, opportunity/pipeline stage, intake responses that are not highly sensitive, service scope, task and document-request status, consent record, appointment history, and a link to the relevant document request.	Passwords, recovery codes, MFA secrets, card/bank-account numbers, passport/ID scans, bank statements, or copies of client documents.
Vaultwarden	Credential vault for accounts Blueprint is explicitly authorized to access or administer.	Login items, TOTP/MFA seeds only when Blueprint owns the administrative workflow, limited secure notes, account owner, purpose, access authorization, recovery owner, and offboarding/revocation instructions.	Client-uploaded general documents, bank statements, identity documents, ongoing case files, or unapproved personal/banking credentials.
Secure document portal / repository	Client upload, request fulfilment, review and controlled access to documents.	Bank statements, identity/citizenship records, tax/legal/financial documents, engagement records, and other requested evidence. Maintain a file/request register and retention category.	Passwords, PINs, one-time passcodes or duplicated CRM operational notes.

Client experience

The client receives one onboarding message from GHL. It directs them to the secure document portal to upload requested files and shows the request list. They should not have to decide whether a bank statement belongs in GHL or Vaultwarden. If credentials are genuinely needed, Blueprint sends a separate, explicit request with the purpose, account name, authorized users, duration of access and revocation process.

What GHL should show

Use GHL as the operational dashboard: onboarding stage, request status (requested / received / under review / complete), owner, due date, last client communication and a link to the secure request. Store only the minimum metadata needed to operate the engagement.

Vaultwarden standard: client collection setup

Vaultwarden should operate as a restricted internal credential service, not as a client portal. A collection is created only where a client has explicitly authorized Blueprint to administer or access specific systems.

Collection naming and structure

- Organization: **Blueprint Global**
- Collection: **Clients / [Client legal name] / Credentials**
- Optional separate collection: **Clients / [Client legal name] / Shared service accounts** - use only if different internal access groups are required.
- Never mix two clients in one collection. Do not use an internal administrator account as a client login.

Required fields on every vault item

- Item name: [System] - [account purpose] - [client legal name].
- URL, account username, client/account owner, and responsible Blueprint owner.
- Access basis: client authorization date and approved purpose.
- MFA and recovery owner: who controls it; never write one-time codes into the vault.
- Access end/review date, plus the revocation or hand-back steps.

Seed only the following items

Item	Create when	Access rule
Client portal administrator	Blueprint administers the client-facing portal.	Blueprint onboarding/admin group only.
Website, hosting or domain administrator	In scope and Blueprint is appointed to administer it.	Named delivery owner plus backup only.
Email/workspace administrator	Approved client administrative scope requires it.	Named administrator only; document client ownership.
Approved third-party platform	A defined service task needs access, e.g., CRM, accounting integration or business manager.	Least privilege and time-bounded where available.

Do not seed

Personal banking logins, payment-card PINs, security questions, one-time passcodes, recovery methods controlled solely by the client, or credentials that Blueprint does not need to perform an approved service. For a bank statement or identity document, use the secure document portal instead.

Setup, access and operating procedure

1. Confirm the data map

Identify each requested data type, its single source of truth, reason for collection, owner, access group, retention category and deletion/return trigger.

2. Configure the document portal

Create the client workspace, default request folders/categories, client upload permissions, Blueprint review permissions, retention rules and activity/audit review. Test a client upload and internal download before launch.

3. Create the GHL operating record

Create the opportunity/onboarding checklist, document-request statuses, owners and due dates. Place a secure link to the document request; do not attach the sensitive source file.

4. Create Vaultwarden collection only if needed

Use the naming standard and assign only the smallest internal group necessary. Verify that the client cannot see other clients and that the delivery team cannot see unrelated collections.

5. Obtain explicit credential authorization

For every credential request, document why it is needed, who will have access, the time period, MFA/recovery approach and offboarding process. Prefer client-controlled delegated access over sharing a primary password.

6. Launch and QA

Run one test client journey: onboarding email, portal invitation, document upload, GHL status update, authorized internal review, expired-access removal and client confirmation.

7. Operate and offboard

Review access at defined intervals and immediately when staff or scope changes. At engagement close, return/transfer access, revoke Blueprint users, close requests, and apply the approved retention/deletion schedule.

Non-negotiable controls

- Unique named accounts for Blueprint staff; no shared staff logins.
- MFA for Blueprint administrators and client portal access where supported.
- Least-privilege groups, documented access approvals, and periodic access review.
- Encrypted backups and a tested restoration procedure for the self-hosted Vaultwarden service.
- A written incident path for suspected misdirected uploads, compromised credentials or lost devices.

Martin approval checklist

Decision	Recommended answer	Martin approval / input
Architecture	Approve the three-system model; no universal repository.	Approve / amend
Secure document tool	Select a dedicated portal/repository with client upload, granular access, retention, auditability and secure sharing.	Choose platform and accountable owner
GHL boundary	CRM metadata, workflow, communications and secure links only; no passwords or high-risk document copies.	Approve / amend
Vaultwarden boundary	Internal credentials only; collection per client only where access is required and authorized.	Approve / amend
Client credential policy	Prefer delegated/client-controlled access. Collect a credential only with documented need, scope, owner, expiry and revocation plan.	Approve policy
Retention and privacy	Define retention schedules, document classification, access reviews and offboarding/deletion responsibility before client launch.	Assign legal/privacy owner

Implementation recommendation

Do not build the client-facing portal inside Vaultwarden. First select and configure the secure document portal/repository, then connect the client journey through GHL and use Vaultwarden only for the small, controlled set of credentials Blueprint needs. This gives clients one clear upload destination and gives the team an auditable, non-redundant operating model.

References checked 10 August 2026

Bitwarden describes organizations and collections as a method of secure sharing of vault items such as logins, notes, cards and identities. Vaultwarden's project describes itself as an unofficial Bitwarden-compatible server and explicitly recommends regular backups for passwords, attachments and other data. The limitations and architecture recommendation in this paper are Blueprint's operational judgment based on those capabilities, not a claim that attachments cannot be encrypted.

Sources: <https://bitwarden.com/help/about-organizations/> | <https://github.com/dani-garcia/vaultwarden> | <https://github.com/dani-garcia/vaultwarden/discussions/6313>