VAULTWARDEN · ADMIN CONSOLE · ZH-TW

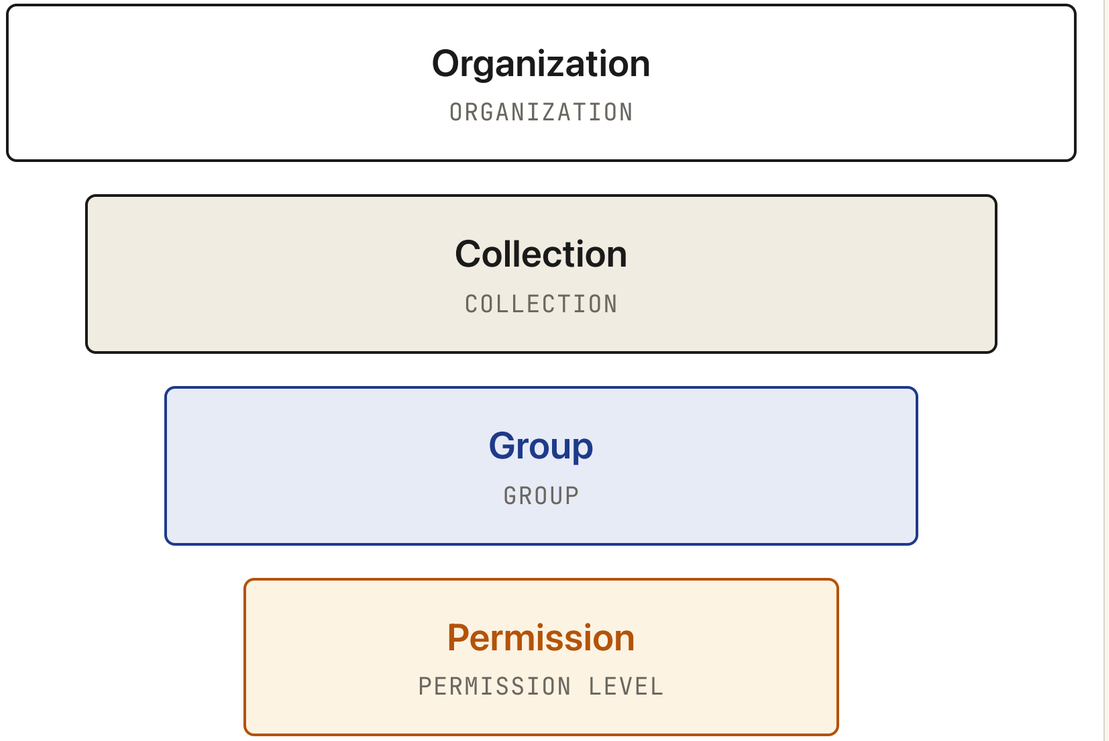
組織管理操作手冊

Admin / Owner — Bitwarden / Vaultwarden 自建組織管理指南

2026 / Q2 · v1.0

vault.example.com
工程部

02 分享模型:四層結構



L1 · CONTAINER

Organization 組織

最外層容器,整個組織的密碼庫。

L2 · WHAT

Collection 集合

把「哪些密碼」分組,是存取控制的最小單位。

L3 · WHO

Group 群組

把「誰」打包,再對 Collection 授權,避免逐人設定。

L4 · HOW

Permission 權限等級

決定「能做什麼」(唯讀 / 可編輯 / 可管理)。

03 三種角色與責任範圍

角色	能做的事	建議人數
Owner	一切設定、刪除組織、移轉擁有權	至少 **2 人**(避免孤兒組織)
Admin	管理成員、Collection、Group;**無法刪組織**	依規模 1–3 人
User	存取被授權的 Collection,依權限等級操作	所有一般成員、bot 帳號

兩條授權路徑,各自獨立

管理層走「角色」(Admin/Owner)取得管理權限;**其他成員走「群組 + Collection」**精確授權、最小特權。 Admin/Owner 角色 不會 自動取得所有 Collection 存取;最敏感的 Collection 需明確指派(詳見第 12 張)。

04 範例 Collections 設計(以 工程部 為例)

以角色為基礎的通用設計,適用各類工程團隊。命名前綴數字僅供排序,無其他含義。

Collection 名稱	用途說明
`00 Everyone`	所有成員皆可存取的公用資訊(Wi-Fi、公用服務帳號)
`10 Admin/Ops`	**最敏感:**伺服器、基礎建設憑證 — 只給 Admin/Owner,不含任何 Group
`20 PM`	專案管理工具帳號(Jira、Confluence 等)
`30 Dev-Shared`	所有開發人員共用(Staging 環境、共享 token)
`31 Frontend`	Frontend 團隊專屬
`32 Backend`	Backend 團隊專屬
`33 App`	App(iOS / Android)團隊專屬
`40 Design`	設計師專屬(Figma、字型授權等)
`90 Automation`	Bot / CI 帳號專屬 — 只給 Bots Group、View items 唯讀

05 Groups × Collection × 權限矩陣

Group	00 Everyone	20 PM	30 Dev-Shared	31 Frontend	32 Backend	33 App	40 Design	90 Automation
PM	E	E	—	—	—	—	—	—
Frontend	E	—	E	E	—	—	—	—
Backend	E	—	E	—	E	—	—	—
App	E	—	E	—	—	E	—	—
Designer	E	—	—	—	—	—	E	—
Bots	—	—	—	—	—	—	—	V

E = Edit items　V = View items　— = 無存取

> `10 Admin/Ops` 不納入任何 Group;Admin / Owner 角色需另行明確指派(見第 12 張)。

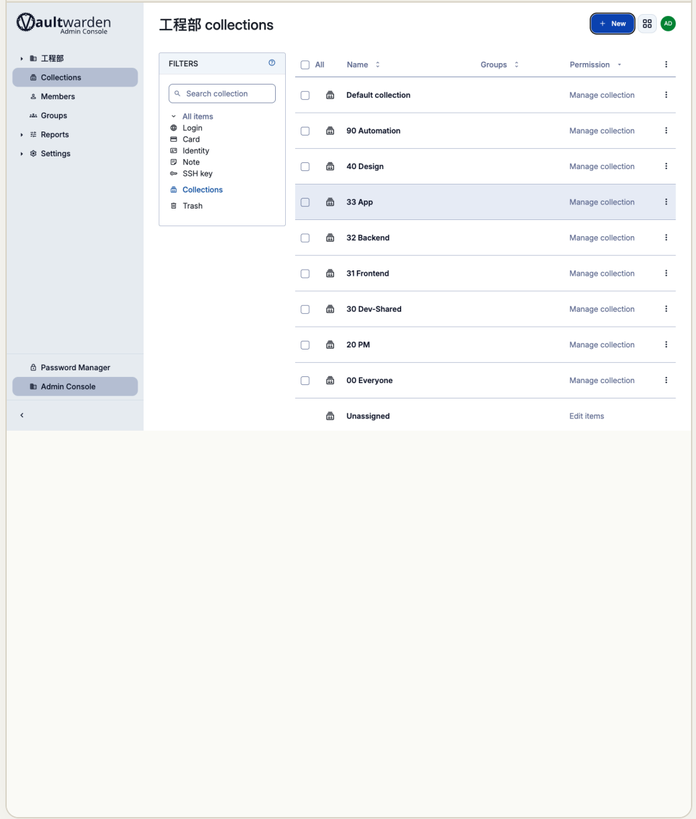
06 建立 Collection

> Admin Console → Collections → New collection

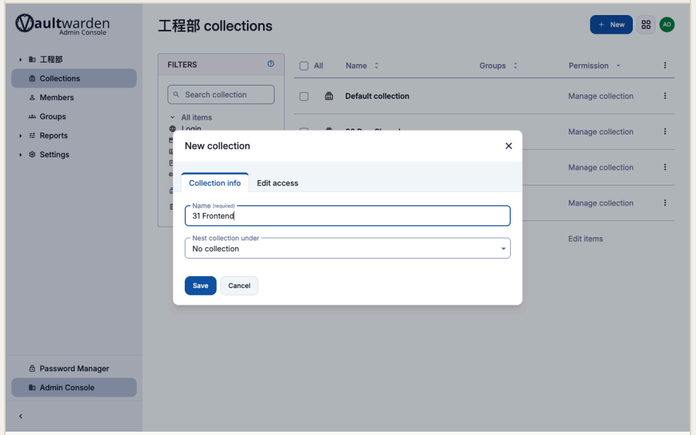
1. 登入 `vault.example.com`,切換到組織 Admin Console。
2. 左側選單 **Collections** → 右上角 **New collection**。
3. 填入名稱(建議用數字前綴排序,如 `30 Dev-Shared`)。
4. (可選)設定巢狀 Collection:名稱以 `/` 分隔父子層。
5. 點擊 **Save**。

建立後於第 10 張的 Group 設定中指派此 Collection 給對應群組。

Collections 清單 [截圖 A1]



New collection 對話框 [截圖 A2]



07 Collection 權限等級詳解

將 Group 或成員指派給 Collection 時,需從下拉選單選擇一個權限等級。

權限等級 (UI 顯示)	說明	適用對象
`View items, hidden passwords`	唯讀;密碼不顯示明文,可自動填入但無法手動複製。	需自動填入但不需看密碼的成員
`View items`	唯讀;可完整查看密碼明文。	需偶爾查閱的唯讀成員
`Edit items, hidden passwords`	可新增、修改項目;密碼不顯示明文。	需維護但不需查看憑證的角色
`Edit items`	可新增、修改、查看密碼 — **一般協作首選**。	團隊日常工作成員
`Manage collection`	Edit items 全部功能 **+ 管理誰能存取 + 刪除此 Collection**。	管理層(謹慎授予)

08 「hidden passwords」的真相 — 軟限制,非硬隔離

「hidden passwords」是 UI 層的軟性限制,不是密碼學意義上的隔離。

技術事實

Bitwarden / Vaultwarden 的架構中,用戶端(瀏覽器 / App)會 **在本機解密所有可存取的 vault 項目** 以支援自動填入。 即使 UI 隱藏密碼欄位,懂技術的使用者仍可透過 **瀏覽器開發者工具或 CLI** 取出明文。

結論

真正的隔離界線是:
「不該知道的人,就不要放進他能存取的 Collection。」

不要用 hidden passwords 代替正確的 Collection 分割設計。

09 Groups 是 Beta 功能,需伺服器端開啟

- Groups 功能目前為 **Beta**,Vaultwarden 預設可能未啟用。
- 若 Admin Console 左側選單看不到 **Groups** 項目,原因是伺服器未設定對應環境變數。
- 此設定需在 `/admin` 伺服器後台或部署設定中調整,**非組織 Admin Console 內操作**(見第 17 張的區分說明)。

啟用方式(由伺服器管理員操作):

```
# 加入 Vaultwarden 環境變數 (.env)
ORG_GROUPS_ENABLED=true

# 重啟服務後生效
docker compose restart vaultwarden
```

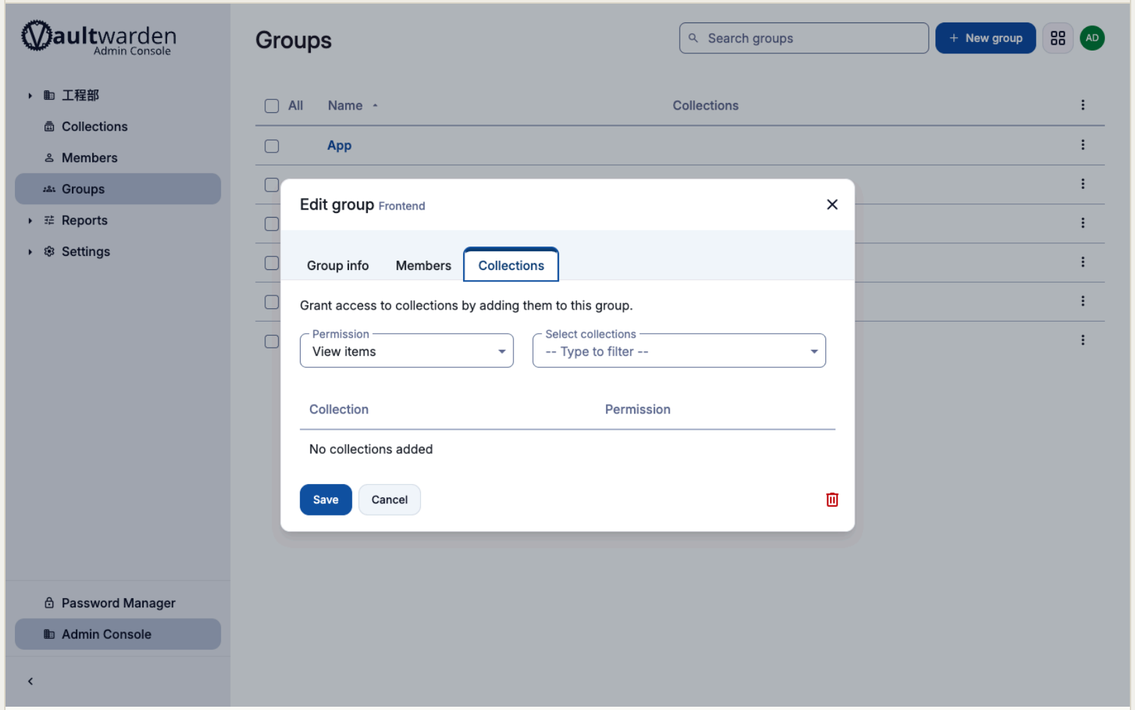
> **啟用後**仍是 Beta:如遇同步異常,先確認此環境變數仍存在並重啟服務。

10 建立 Group 並授權 Collection

> Admin Console → Groups → New group

1. Admin Console 左側選單 **Groups** → **New group**。
2. 填入群組名稱(如 `Frontend`)。
3. 切換到 **Collections** 分頁。
4. 搜尋並選取要授權的 Collection(如 `00 Everyone`、`31 Frontend`、`30 Dev-Shared`)。
5. 對每個 Collection 從右側下拉選擇對應 **權限等級**(參照第 5 張矩陣)。
6. 點擊 **Save**。

New group → Collections 分頁　[截圖 A4]



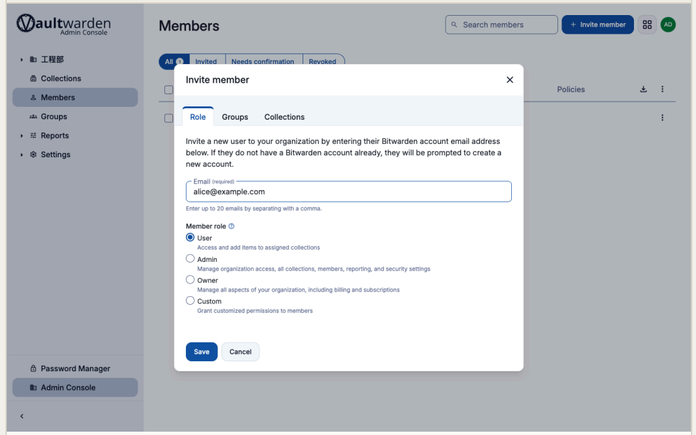
11 邀請成員加入組織

> Admin Console → Members → Invite member

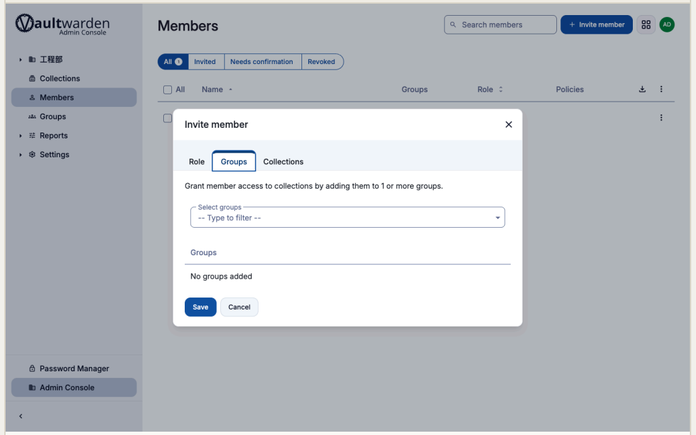
1. Admin Console **Members** → **Invite member**。
2. **Email** 欄位輸入成員 email(如 `alice@example.com`),可一次填多個。
3. **Role** 分頁:一般成員選 **User**;管理層選 **Admin**(Owner 角色另行在成員頁設定)。
4. **Groups** 分頁:勾選該成員所屬的 Group(如 `Frontend`)。
5. 點擊 **Send**。

> 需伺服器已設定 SMTP,否則邀請信不會送出 — 可手動複製邀請連結提供給成員。

Invite member · Role [截圖 A7]



Invite member · Groups [截圖 A8]



12 最敏感 Collection 的管理層存取

`10 Admin/Ops` 不納入任何 Group;Admin/Owner 需 **另行設定** 才能存取。以下兩種做法:

A · 推薦

明確指派 — 最小特權

邀請管理層成員時,切換到 **Collections** 分頁,手動加入 `10 Admin/Ops`,並選擇 **Manage collection** 或 **Edit items**。

- 每位管理員的存取可單獨開關
- 符合最小特權原則,稽核清楚
- 新管理員上線需明確走流程

B · 全域開關

較粗糙的快捷做法

組織 **Settings → General** → 開啟 「Owners and admins can manage all collections」。

- 所有 Admin/Owner 自動取得全部 Collection 管理權限
- 無法針對個別管理員做精細限制
- **不符合最小特權原則**

建議:優先選做法 A;僅在確實需要所有管理員存取全部 Collection 時才用做法 B。

13 邀請三階段:Invite → Accept → Confirm

ADMIN
Invite member

→

MEMBER
收信並 Accept

→

ADMIN
Confirm(必須手動)

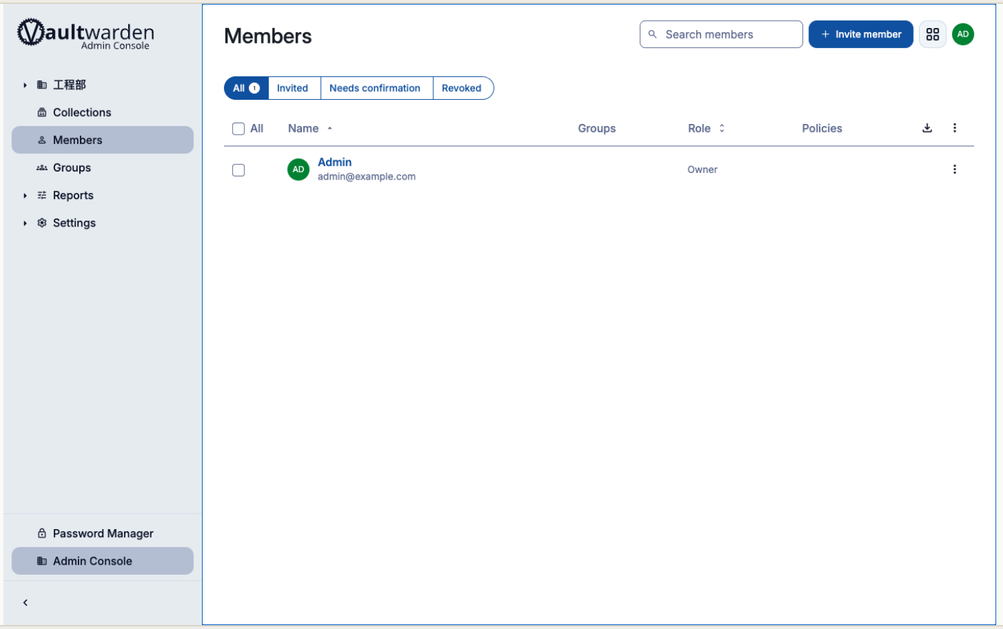
Confirm 的意義

Confirm 是把 **組織加密金鑰(Org Key)** 用新成員的公鑰加密後分享給他。 這是 Bitwarden 的零知識安全設計,**伺服器(含 SMTP)無法代勞**。

常見遺漏

管理員傳送邀請後 **忘記回來 Confirm**,成員進去卻看到空白 vault。 未 Confirm 前,成員看不到任何組織共享內容。

Members 清單(範例)　[截圖 A6 / A9]



14 至少兩位 Owner — 避免組織孤兒

> **風險**
>
> 若 **唯一** 的 Owner 離職或帳號無法存取,組織可能 **永久失去管理能力**(無法刪除、無法移轉) — 因為 **Owner 權限無法由 Admin 授予**。

設定第二位 Owner

1. Admin Console **Members** → 找到目標成員(已 Confirmed)。
2. 點擊成員旁的設定選單 → **Edit** → Role 改為 **Owner** → Save。
3. 確認該成員已 **明確授予** `10 Admin/Ops` Collection 存取(同第 12 張)。

維運建議

- 維持 **至少 2 位 Owner**,記錄於組織文件中
- Owner 帳號 **啟用強主密碼**
- Owner 帳號 **強制啟用 Two-step Login(2FA)**
- 人事異動時即時盤點 Owner 名單

15 Bot 帳號的最小特權設計

> Vaultwarden **沒有** Service Account 或機器帳號概念 (那是 Bitwarden Secrets Manager 的功能,尚未在 Vaultwarden 實作)。
> Bot 使用一般 User 帳號,**但必須嚴格隔離**。

- [x] **專屬 Collection**
  建立 `90 Automation`,只放 bot 需要的憑證。
- [x] **專屬 Group**
  `Bots` Group 只授權 `90 Automation`,權限 **View items**(唯讀)。
- [x] **獨立帳號**
  每支 bot 一個帳號(如 `bot@example.com`),便於稽核與個別撤銷。
- [x] **不加入其他 Group**
  Bot 帳號不放進 `Everyone` 或任何團隊 Group。
- [x] **絕不給 Admin/Owner 角色**
  Bot 只能是 **User**,角色不可上升。
- [x] **憑證保存於 Secret Manager**
  Bot 主密碼與 API key 存入雲端 Secret Manager(如 GCP Secret Manager),**不寫死在程式碼**。

16 Bot 如何用 CLI 存取 Vault

使用 Bitwarden CLI(`bw`)搭配 **個人 API key** 登入:

```
# 設定 API key 環境變數
export BW_CLIENTID="user.xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
export BW_CLIENTSECRET="xxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

# 以 API key 登入(跳過互動式主密碼輸入)
bw login --apikey

# 解鎖 vault(需主密碼解密本機金鑰)
export BW_SESSION=$(bw unlock --passwordenv BW_PASSWORD --raw)

# 取得項目
```

為何可行

Vaultwarden 保留 **標準密碼登入**(未開啟 SSO_ONLY), 因此 API key + 主密碼的組合可正常運作。

機密管理

主密碼(`BW_PASSWORD`)與 API key 應從 **Secret Manager 動態注入**, 不寫入程式碼或版本控制。

17 兩個管理介面,用途不同

這兩個介面常被混淆,但職責完全不同。

	`/admin` 伺服器後台	Admin Console(組織管理)
存取路徑	`vault.example.com/admin`	`vault.example.com` → 組織 → Admin Console
保護機制	IAP + `ADMIN_TOKEN`	組織 Owner / Admin 帳號
用途	伺服器設定、使用者封鎖 / 刪除、SMTP 診斷、發送邀請(伺服器層)、檢視系統狀態	Collection 管理、Group 管理、成員邀請 / Confirm、組織設定
日常操作	**否**(由伺服器管理員維護)	**是**(Owner / Admin 日常使用)

> **結論:** 日常的組織管理(Collection / Group / 成員)一律在 Admin Console 操作; `/admin` 保留給伺服器層維護。

18 成員離職 / 帳號撤銷流程

1. Admin Console **Members** → 找到離職成員。
2. 勾選 → **Remove**,或從設定選單選 **Revoke access**(立即失效,無需等待)。
3. 評估是否需要 **輪換共享密碼**(見右側)。
4. 確認 `90 Automation` 中的 bot 帳號是否也需同步更新(若離職者知道 bot 主密碼)。

> **Group 設計的好處:**移除成員後,Collection 存取自動隨之解除,**無需逐一移除 Collection 指派**。

密碼輪換判準

- 若成員曾有 **Edit items** 或更高權限,視情況輪換他接觸過的 Collection 中的憑證。
- `10 Admin/Ops` 中的憑證在 **管理層異動時應一律輪換**。
- 共享 token、API key、伺服器密碼 — 優先輪換。
- 個人 SaaS 帳號(只有該成員使用) — 通常停用即可。

19 日常 SOP 速查表

SOP 01 新人上線

1. 確認 SMTP 正常(或準備手動傳送邀請連結)。
2. Invite member → 填 email、選 Role(**User**)、選 Group → Send。
3. 等成員 Accept → 回 Members 頁面 **Confirm**。
4. 通知成員可開始使用。

SOP 02 定期維運

- **每季**檢視 Group × Collection 矩陣,確認符合最小特權。
- **每年或人事異動時**盤點 Owner 名單,維持至少 2 人。
- **Offboarding 當天**執行 Revoke + 評估密碼輪換。
- Groups 異常時,確認 `ORG_GROUPS_ENABLED=true` 並重啟服務。

求助信箱
it-support@example.com

VAULT 網址
vault.example.com

20 管理原則總結與聯絡方式

01 最小特權

只給需要的 Collection,只給需要的權限等級。

02 Group 優先

透過 Group 授權,避免逐人設定造成遺漏。

03 Confirm 不能忘

邀請後必須手動 Confirm,成員才能看到共享內容。

04 兩位 Owner

永遠維持至少兩位 Owner,組織才有保險。

05 隔離 > 隱藏

hidden passwords 是軟限制;真正的隔離靠 Collection 設計。

求助 / 回報問題	VAULT 網址	文件版本
it-support@example.com	vault.example.com	v1.0 · 2026 Q2