

증빙 — 감사 보고서 표 · 시각별 실행 로그 · 교차검증 판정

본편에 인용한 수치의 원문입니다. 운영 중인 서비스라 취약점의 필드명·키 종류·요청 형태와 계정 식별자는 가렸습니다.

증빙 1. 운영현장 원문 (COMPANY.md · 영문 원본 발췌)

본편 ②의 요약은 아래 원문을 우리말로 간추린 것입니다. 데모 계정 주소는 가렸습니다.

VI One — Company Operating Charter

> Established 2026-07-14 by CEO decision. This file is the standing instruction for all AI officer agents working on VI One.

Structure

Role	Holder	Mandate	Escalates to CEO when
CEO	Sangwoo (human)	All final decisions: release, pricing, scope	—
COO	AI agent team	Product quality, UAT, operations, runbooks	Any P0/P1 defect, release risk
CIO	AI agent team	Infra, Supabase, security, data protection	Security hole, data-loss risk, outage
CFO	AI agent team	Pricing, IAP/subscription integrity, costs	Revenue leak, billing defect, cost spike
CMO	AI agent team	Store listing, marketing assets, reviews	Brand/legal risk, listing rejection

Operating rules

- Each officer commands up to 100 worker-agent slots, dispatched in parallel batches per task. Workers report to their officer; officers consolidate and report to the CEO in writing.
- Officers never make irreversible decisions (App Store submission, payments, data deletion, outbound messages to real customers) — CEO clicks those.
- Every task ends with a written report in `reports/` (date-prefixed). Severity scale: **P0** blocker · **P1** major · **P2** minor · **P3** polish.
- Production data guardrails: demo account `the App Store review demo account` must stay intact (App Store review depends on it). Test records use the `UAT\_` prefix and are cleaned up. No live SMS/calls to real numbers. Never invoke account deletion on the demo account.
- Core product values (CEO-set, do not violate): continuous customer communication (SMS/WhatsApp/KakaoTalk/phone stays in), AI answers FAQ-only with human fallback, AI features gated to Pro/Business.

증빙 2. 통합 UAT 보고서 제4절 — 수렴된 결함 9건

심각도 집계 P0 2 · P1 2 · P2 4 · P3 1 = 9건. 재현 가능한 세부는 가린 상태입니다.

ID	Issue	Who found it	Severity	Status
1	**Paid tier is free for the taking** — any logged-in user can set their own `the plan field (name withheld)` with the app's public key and unlock Pro. Server verification is real but lands in a user-writable cell.	CIO + CFO (live-verified)	**P0**	✅ Fix staged — migration `0002` + `iap-verify` v3
2	**Purchases 500 in production** — App Store keys (`ASS_`) not set, so `iap-verify` errors. Nobody can pay; the Apple reviewer hits the same wall.	Restaurant owner (live) + CIO	**P0**	🕒 You set 4 secrets (Runbook A)
3	**Apple renewal/refund webhook is forgeable** — no signature check; a forged			

notification could be accepted (request shape withheld). | CIO + CF0 | **P1** |  Fix staged – `appstore-notifications` v3 (JWS verify)* |
 | **4** | **Messaging dead on the demo account** – no inbound number wired + AI auto-reply OFF, so the headline "소통" value looks broken to a reviewer. | Restaurant owner (live) | **P1** | 
 You set up demo account (Runbook D) |
5	**AI endpoints have no server-side tier gate** – free users can call `ai-chat` directly and burn your OpenAI spend.	CF0 + C00	P2	 Fix staged – `ai-chat` v6 gate
6	**Inbound SMS webhook unauthenticated** – spoofed inbound could pollute the CRM (toll-fraud risk); auto-reply threshold set too low.	CIO	P2	 Fix staged – `msg-inbound` Twilio-sig + 0.6
7	**IAP sandbox accepted in prod / no purchase-to-account binding** – sandbox receipts were accepted in production.	CIO + CF0	P2	 Fix staged – `iap-verify` v3
8	**Repo drifted from production** (functions + schema); DB migration file was a stub.	C00 + CIO	P2	 Live sources pulled into repo
9	Owner-experience polish: stale "today" screen, VIP tags empty, no restaurant onboarding, `usage\_minutes` client-writable.	Owner + CIO	P3	☐ Backlog (not launch-blocking)

조치상태 (실행 로그 기준 갱신)

조치상태는 아래 실행 로그(증빙 3) 기준으로 다음과 같습니다. 1번 · 5번 · 6번 · 7번 운영 반영 완료 (2026-07-14 02:35~03:02)
 2번 · 4번 CEO 조치 항목 — 자격증명·계정 설정 3번 후속 조치 항목 (03:42 로그에 '재개 필요'로 기록) 8번 저장소를 운영 기준으로 갱신해 해소 9번 백로그 (출시 비차단) 표 원문의 Status 칸은 감사 시점 값이라 이후 배포를 반영하지 않습니다. 재현 방법은 공개하지 않습니다.

증빙 3. 시각별 실행 로그 — 누가 언제 무엇을 했는가

근태 기록 중 자동 생존신호를 뺀 실작업 13건 전량(2026-07-14, 로그 표기 시각).

```
00:35 C00 풀 기능 UAT 화이트박스 스왑(전 탭+엡지함수+스키마)
      ↳ P0 2·P1 2·P2 6·P3 6 발견, 리포트 제출
00:52 CIO 백엔드 보안감사(RLS·grants·advisors 라이브)
      ↳ RLS 19테이블 OK, entitlement 클라 쓰기 P0 확인
01:10 CF0 구독/IAP 매출무결성 리뷰
      ↳ RI-1 P0: plan 클라 조작 가능
01:40 C00 레스토랑 오너 실시나리오 테스트(라이브 데모계정)
      ↳ AI응대 우수, 결제500·문자미연결 dealbreaker
02:15 CIO 엡지함수 4종 보안 하드닝 스테이징
      ↳ iap-verify·ai-chat·appstore·msg-inbound 패치
02:35 CIO iap-verify v4 운영 배포(서버 권한으로 쓰기 전환)
02:41 CIO 0002 보안잠금 마이그레이션 적용
      ↳ plan 트리거+grant 회수
02:48 CIO 익스플로잇 재검증 중 트리거 SECURITY DEFINER 버그 발견
      ↳ plan 조작이 안 막힘 → 즉시 수정
02:55 CIO guard 트리거 SECURITY INVOKER로 수정+데모 plan pro 원복
      ↳ 재검증: business 시도→pro 유지 확인
03:02 CIO ai-chat v7·msg-inbound v3 운영 배포
      ↳ 티어게이트·Twilio 서명검증 라이브
03:20 CM0 App Store 리스팅 패키지 작성(KR/EN)
      ↳ 이름·설명·키워드·스샷카피·프라이버시
03:35 C00 유료 Starter SKU 제거(페이월 정리)
      ↳ Starter=무료
03:42 CIO appstore-notifications 재조회 방식 하드닝(스테이징)
      ↳ 세션 한도로 중단 — 재개 필요
```

증빙 4. 근태 로그 집계 — 계속 장치가 실패했음을 보여주는 숫자

총 기록 609건 기간 2026-07-14 ~ 2026-08-08
담당별 CIO 157 · C00 152 · CF0 150 · CM0 150
상태별 working 596 · done 11 · error 1 · blocked 1
자동 생존신호(heartbeat) 596건 / 실제 작업 기록 13건

증빙 5. 같은 방법의 두 번째 적용 — 정부지원사업 조사 교차검증

개발과 무관한 업무에 같은 역할분리·교차검증 구조를 적용한 사례입니다(2026-09-09).

대상: 보고서 20건 (A1~A10, B1~B10) · 작성 2026-09-09 · 교차검증 에이전트 1개
판정 기호 기계적 계수 — 확인 43 · 수정 필요 20 · 판단 불가 5
(범례 줄과 절 제목이 포함돼 실제 판정 건수보다 두세 건 많을 수 있습니다)
부록 「각 보고서에 반영해야 할 정정 목록」 9행

교차검증 에이전트가 잡아낸 대표 오류 (원문 발췌) — 센터는 중지 사실을 공고에 정확히 게시하고 있었고, 확인하지 않은 것은 제 AI 보고서였습니다.

서울지식재산센터 「소상공인 IP출원(상표출원) 지원사업」 — ⚠️ **수정 필요 (중대)**

⚠️ 핵심: **서울센터 접수는 중지 상태다. 지금 신청할 수 없다.**

RIPC 통합 안내 페이지(`https://pms.ripc.org/smallbiz`) 원문:

> **「2026년 서울 소상공인 IP(상표)출원 지원사업 접수 중지 안내」
> · 중지일: 2026. 8. 25.(화)
> · 중지 사유: 예산 지원 규모 초과 접수에 따른 조기 마감**

같은 페이지의 타 센터 현황(비교용):

- 경기북부: 중지 2026-04-30 (동일 사유)
- 경기남부: 마감 2026-09-01 ("2026년 사업예산이 소진되어")
- 경남: 마감 2026-07-22
- **부산: 재오픈 2026-09-07 09:00** ← 잔여예산 회수 시 재개 사례가 실제로 있음

****A10 §0 표의 "순위 1 / 지금 바로 / 사장님 전화+본인인증"은 성립하지 않는다.**** A10은 스스로 "ipseoul.kr 접속 차단"·"서울센터 잔여예산 확인 필요"라고 단서를 달았으나, 결론 표에서는 그 단서를 지우고 1순위 즉시 실행으로 올렸다. ****사장님이 이 표만 보고 움직이면 헛수고한다.****

이 증빙에는 고객 개인정보·API 키·비밀값·계정 식별자를 포함하지 않았습니다. 표·도표는 원본 텍스트를 그대로 옮겨 조판한 것이며 원본 화면 캡처가 아닙니다.