AI.SHOKU / PEOPLE MEET OPPORTUNITY

Service & deployment manual

English / Native PHP & MySQL / Approved-design release

Version 1.1.0-rc1 • 22 September 2026

> For your own Linux server, MySQL database and HTTPS domain.

Contents

01 Runtime and release boundaries

02 Install on your Linux server

03 Domain, HTTPS and portal sessions

04 AI, email and optional voice

05 Workers, maintenance and safe intervention

06 Data, retention, backup and upgrades

07 Acceptance before real candidate processing

Local verification is distinct from production acceptance. Read the release gate record before processing real candidate data.

Runtime and release boundaries

Native PHP 8.3+, PHP-FPM, PDO MySQL and MySQL 8.4 are the target runtime. Linux must provide sodium, openssl, fileinfo, curl, mbstring, DOM/XML, ZIP and iconv; the document pipeline also needs pdftotext, GNU timeout and ClamAV. This package has no third-party Composer package dependency and no Python/Node backend.

The approved visual system is connected to PHP APIs and server authorization. Published evidence, applications, interviews, notifications and audits are persisted in 32 MySQL tables, including the migration ledger. The schema remains migration 001.

Code and local test evidence are provided, not a production certification. Target MySQL, real IdP-free native MFA flow over HTTPS, SMTP, AI, voice, scanning, load, disaster recovery and accessibility need acceptance on your host. No live server or domain has been changed by preparing this package.

Install on your Linux server

1. Read docs/SETUP_LINUX_EN.md or SETUP_LINUX_JA.md before running commands. The Ubuntu helper targets 24.04/PHP 8.3 and does not replace an existing MySQL server.
2. Place code outside the public web root. Use /var/www/aishoku/public as document root; make code read-only to the web account. Keep private storage at /var/lib/aishoku. Never use chmod 777.
3. Generate .env once using setup with your HTTPS origin. Preserve APP_KEY; losing or changing it makes encrypted records unreadable. Store secrets privately, not in source control or chat.
4. Have your DBA create a dedicated UTF-8 database and separate runtime/migration accounts. Run the initial migration once into an empty database. Never reset an existing customer database to resolve a migration error.

```
cd /var/www/aishoku
sudo php bin/console setup --url=https://jobs.example.com --environment=production
# Edit .env privately; replace the placeholder domain.
sudo php bin/console migrate --credentials-file=/etc/aishoku/migration.env
sudo -u www-data php bin/console preflight
```

> The above domain is a placeholder, not a published Ai.shoku address. Follow the full guide for ownership, permissions and migration-account files.

Domain, HTTPS and portal sessions

1. Point your DNS records at the host. Bootstrap certificate issuance, then enable the reviewed Nginx or Apache/FPM template with the correct PHP socket and certificate paths. Preserve unrelated hosted sites.
2. Allow only public/index.php as the executable web entry point. Keep .env, app, database, tests and storage outside public access.
3. Set APP_URL and, optionally, the four portal URLs. Optional portal URLs include their portal path. Secure, HttpOnly, SameSite cookies and server sessions are purpose-scoped. Same-domain paths are not separate browser origins.
4. Run deploy/verify-domain.sh against the actual HTTPS origin, then manually test login and workflows on desktop and an iPhone/Android browser. This check does not publish or modify anything.

```
sudo nginx -t
sudo systemctl reload nginx
sudo systemctl reload php8.3-fpm
bash deploy/verify-domain.sh https://YOUR-REAL-DOMAIN
```

> Readable server HTML, manual links and a timed recovery message now replace the old endless preview spinner. They do not make an unhosted file into a live application.

AI, email and optional voice

Setting group	Required configuration
AI	AI_MODE=live; AI_BASE_URL; AI_MODEL; AI_API_KEY; AI_DAILY_CALL_LIMIT
Mail	MAIL_TRANSPORT=smtp; MAIL_FROM; SMTP_HOST; SMTP_PORT; SMTP_ENCRYPTION; SMTP_USERNAME; SMTP_PASSWORD
Help	AI_HELP_ENABLED=true only after provider approval; default false
Voice	VOICE_ENABLED=true; STT_MODEL; TTS_MODEL; TTS_VOICE
Notice	PRIVACY_CONTACT; AI_PROVIDER_DISCLOSURE; DATA_REGION_DISCLOSURE

AI_BASE_URL must implement the supplied JSON chat and optional speech contracts. Compatibility labels alone do not prove this. JDs, resumes and answers are untrusted content. Model output must pass schema, ID and quotation checks; deterministic code controls scores and permissions. Human review remains required.

Configure sender authentication (SPF, DKIM, DMARC) with your mail provider. Use an exact recipient allowlist in staging. SMTP acceptance is not proof of inbox delivery. Bounce/complaint ingestion is not a completed provider integration.

No PSTN dialing, full-duplex voice agent, dynamic interview follow-ups, external-calendar sync, SAML/OIDC/SCIM, billing or ATS connector is delivered as a completed module.

Workers, maintenance and safe intervention

Enable the supplied systemd worker and minute scheduler. Both use the same private configuration, stable encryption key, database and persistent storage. Check status and logs after startup. The ops portal shows task states and logical mail status, not provider delivery guarantees.

```
sudo systemctl enable --now aishoku-worker.service
sudo systemctl enable --now aishoku-scheduler.timer
sudo systemctl status aishoku-worker.service
sudo journalctl -u aishoku-worker.service -n 100
```

Tasks have deduplication keys, leases, bounded retries and dead states. Review the error code before retrying. External work is not universally exactly-once. Uncertain SMTP outcomes must be reconciled before resend.

Monitor old queued tasks, dead/uncertain messages, disk capacity, DB health, processes, certificate expiry, API latency and quotas. /healthz checks the entry point; /readyz checks a DB connection, not every dependency. External alerting is not bundled.

Data, retention, backup and upgrades

Approved job/profile versions, answers, reviews and selected audit/evidence records are immutable. Tenant authorization is in PHP policy queries; no MySQL row-level-security feature is claimed. Personal text and raw files are encrypted using the application key, but metadata and identifiers are not all encrypted.

Preview raw-document expiry with documents:purge before adding --apply under an approved policy. This does not erase every published profile or interview. A deletion request suspends processing and requires authorized manual review.

Back up the database, encrypted private files and APP_KEY as a coordinated recoverable set. Never place the key in the same unrestricted archive. Test restores into an isolated host with outbound communications blocked. Revalidate triggers/definers, permissions, decryption and queues. Record RPO/RTO rather than assuming them.

> For an upgrade from PHP 1.0.0-rc1, retain your existing .env, APP_KEY and storage. There is no new schema migration in 1.1.0-rc1. Re-run acceptance and restart workers. This is not an automatic migration of the older Python/PostgreSQL build or the existing SES site.

Acceptance before real candidate processing

1. Run the disposable *_test MySQL suite; verify migration, triggers, DML-only account access, uniqueness and concurrent booking/worker behavior on your actual database version.
2. Test real-domain HTTPS, browser sessions, portal boundaries, MFA, CSRF, verification/reset and account revocation.
3. Execute a complete synthetic recruitment journey in EN and JA; validate email receipt, timezones, real microphone handling and human review.
4. Evaluate representative Japanese/English resumes and jobs with human-labelled matching/grade datasets; test insufficient evidence and protected-attribute sensitivity. Unit arithmetic tests do not establish model quality.
5. Complete vulnerability/dependency review, file isolation/scanning tests, privacy/legal review, accessibility/mobile UAT, load tests and a restore drill. Assign named release owners and attach the evidence.

Use docs/PRODUCTION_GATES.md and docs/TEST_RESULTS.md as the release record. This single-host reference does not claim high availability or unlimited enterprise scale.