Penetration Test — Summary

PYREXA Inc · May 2026 · Confidential

Engagement status

PYREXA has scoped an external grey-box penetration test covering the customer portal, admin console, API surface, OAuth callbacks, and AI prompt-injection boundaries.

Vendor selection is in progress (current candidate set: Cure53, NCC Group, Trail of Bits, Bishop Fox). Engagement target window: pre-public-launch.

Internal pre-checks (the items the security team controls before sending to a vendor) are tracked in docs/security/PENTEST_CHECKLIST.md within the PYREXA engineering repository and reviewed monthly.

Threat model focus areas

Multi-tenant isolation (every business_id filter, RLS policies, JWT sub-business binding).

OAuth callbacks (Meta, Google Calendar, Stripe Connect) — state forgery + replay.

Webhook signature verification (Stripe, Resend, Twilio, Meta) — replay, stripping, missing-secret fail-closed.

AI prompt injection — exfiltration of system prompt, persona pivot.

At-rest encryption — envelope format, rotation procedure, key-loss recovery.

Rate limiting — per-replica defeat, distributed bypass.

Voice + SMS abuse — toll fraud via /onboarding/demo-call and /voice/test-call.

TOTP recovery codes — single-use enforcement, race conditions.

PII in logs — verification that scrubSecrets coverage extends to Sentry breadcrumbs.

Per-business kill switch — verifying a paused tenant truly cannot trigger any auto-reply path.

Remediation SLA

Critical: 24 hours. High: 7 days. Medium: 30 days. Low: next release. Informational: tracked, not blocking.

Continuous testing posture

Internal automated security checks: aiDefence injection scans on every inbound request, dependency scanning via npm audit on every PR, secret scanning via gitleaks on commit, branch-protection enforced merge-via-PR.

Report cadence

On completion, this PDF is replaced with the vendor's executive summary (redacted of reproduction-step detail). Full findings remain available to enterprise customers under NDA via security@pyrexa.ai.

This document represents PYREXA's current compliance posture. For executed agreements, audit attestations, or vendor-specific addenda, contact security@pyrexa.ai.