SECURITY PROGRAM

Information Security Overview

For vendor security assessments, CISO reviews, and enterprise procurement teams.

Access Control | Incident Response | Vulnerability Mgmt | Business Continuity | Vendor Risk

01 Security Governance

Privedge maintains a security-first engineering culture. Security decisions are owned at the engineering leadership level with no separate security team — every engineer is responsible for the security of the code they ship.

SECURITY OWNER
CTO / Engineering Lead

REVIEW CADENCE
Quarterly security review + ad hoc post-incident

SECURITY TRAINING
All engineers: OWASP Top 10, secure coding, phishing simulation on hire and annually

CODE REVIEW
Mandatory peer review for all PRs. Security-sensitive changes require lead sign-off

DEPENDENCY SCANNING
Automated via GitHub Dependabot + npm audit on every CI run

SAST / SECRETS SCANNING
GitHub Advanced Security — secret scanning + code scanning on all branches

02 Access Control

Access to production systems follows a strict least-privilege model. No Privedge employee has programmatic access to customer prompt data — this is enforced by architecture, not policy.

CONTROL	POLICY
`Customer prompt data`	ZERO employee access. V8 isolate model: data exists only in-memory per request. No persistent store to access.
`Audit metadata (Pro/Enterprise)`	Access restricted to on-call engineers for incident response. Logged and reviewed quarterly.
`Production infrastructure (Cloudflare)`	MFA enforced. SSO via identity provider. Role-based: deploy access separate from config access.
`Customer API keys`	Stored in Cloudflare Workers Secrets (AES-256). Not accessible to Privedge engineers in plaintext.
`Source code`	MIT open-source. Public read. Write access: named engineers only, protected main branch, required reviews.
`Internal systems (GitHub, Cloudflare dash)`	Phishing-resistant MFA (hardware key or passkey). Access reviewed on personnel change.

03 Change Management

All production changes go through a controlled deployment pipeline. No direct production access — all changes via CI/CD.

1. **Branch:** All changes on feature branches off `main`
2. **PR + review:** Mandatory peer review. Security-sensitive paths require lead approval
3. **CI checks:** Automated tests, SAST, dependency audit, type checking must pass
4. **Staging deployment:** Changes deploy to staging environment for smoke testing
5. **Production deploy:** Manual trigger by authorized engineer via Wrangler / Cloudflare CI
6. **Rollback:** Previous Worker version instantly restorable via Cloudflare dashboard (<30s)

> **Emergency hotfix:** Same process, abbreviated review window (30 min minimum). Post-incident review required within 24h.

04 Incident Response

Privedge maintains an incident response plan aligned with GDPR Art. 33 notification timelines and NIST CSF principles.

T+0 — Detection
Incident detected via monitoring, customer report, or automated alert. On-call engineer paged.

T+1h — Triage
Severity classification (P0–P3). P0/P1: immediate escalation to all engineers + leadership.

T+4h — Containment
Affected systems isolated or rolled back. Attack vector identified and closed if possible.

T+24h — Customer notice
Affected customers notified if personal data involved. Initial notice within 24h of confirmed breach.

T+72h — DPA notification
Supervisory authority notified per GDPR Art. 33 if applicable. Incident report issued to affected customers.

T+7d — Post-mortem
Full RCA published internally. Corrective actions tracked to closure. Pattern analysis for prevention.

05 Vulnerability Management

DEPENDENCY SCANNING

Automated daily via Dependabot. Critical CVEs patched within 24h. High within 7 days.

PENETRATION TESTING

Annual third-party pentest targeting Worker endpoints, auth flows, and tokenization logic. Report available under NDA.

RESPONSIBLE DISCLOSURE

Public security.txt at privedge.io/.well-known/security.txt. Bug reports to security@privedge.io. 90-day disclosure window.

INFRASTRUCTURE CVES

Cloudflare patches V8 / runtime vulnerabilities. Privedge inherits Cloudflare's patching SLA: critical within 24h.

SAST

GitHub Code Scanning (CodeQL) on every PR. Results reviewed before merge.

ATTACK SURFACE

Minimal by design: single Worker endpoint, no admin panel, no database, no persistent auth sessions.

06 Business Continuity

Privedge inherits Cloudflare's global network resilience. The product has no single point of failure — requests are served from the nearest of 300+ edge nodes.

METRIC	TARGET	NOTES
Availability SLA	99.9% (Pro), 99.99% (Enterprise)	Backed by Cloudflare network SLA
RTO (Recovery Time Objective)	< 30 seconds	Instant Worker rollback via Cloudflare dashboard
RPO (Recovery Point Objective)	N/A — no stateful data	No persistent prompt storage to recover
Geographic failover	Automatic	Cloudflare Anycast: nearest healthy node serves request
DDoS mitigation	Unlimited (Cloudflare)	Cloudflare Magic Transit absorbs volumetric attacks
Planned maintenance	Zero-downtime	Worker deploys are atomic — old version active until new version healthy

07 Sub-processor Register

Privedge engages the following sub-processors. Customers are notified of any changes with 30 days advance notice. Customers may object within 14 days of notice.

SUB-PROCESSOR	PURPOSE	LOCATION	CERTIFICATIONS
Cloudflare, Inc.	Edge compute runtime (Workers) — processes all requests	Global (EU region for EU customers)	SOC 2 T2 · ISO 27001 · HIPAA · PCI DSS L1
Cloudflare, Inc.	Audit log storage (R2) — Enterprise tier only, no prompt content	EU (configurable)	SOC 2 T2 · ISO 27001
Cloudflare, Inc.	API gateway, DDoS mitigation, TLS termination	Global	SOC 2 T2 · ISO 27001

Note: In self-hosted deployments, Privedge (the company) is NOT a sub-processor. All processing occurs in the customer's own Cloudflare account. The above applies to cloud-mode (privedge.io) customers only.

08 Data Residency & Portability

PROMPT DATA RESIDENCY

N/A — prompt content is never stored. Processed in-memory at the nearest Cloudflare edge node.

AUDIT LOG RESIDENCY

EU customers: EU Cloudflare R2 bucket. Configurable on Enterprise plan.

CROSS-BORDER TRANSFERS

Covered by Cloudflare's SCCs (Standard Contractual Clauses) and adequacy decisions. Available on request.

DATA EXPORT

Audit logs exportable as JSON or CSV at any time. No vendor lock-in — logs contain no proprietary format.

DATA DELETION

On contract termination: all audit logs deleted within 30 days. Written confirmation provided.

SELF-HOST

MIT license. Deploy in your own Cloudflare account for complete data sovereignty. Zero data leaves your account.