

Security Overview

The controls behind Heyou's product — tenant isolation, EU data residency, encryption, AI-call PII minimization, SSO/MFA, third-party penetration testing, and our incident-response posture.

Version 1.0

Effective 10 May 2026

Last updated 10 May 2026

heyou.io/security/

1. Certifications and Frameworks

- **ISO/IEC 27001:2022** — Certified. SII Certificate No. 1127825 (ANAB-accredited), IQNET registration IL-1127825, valid 23 Apr 2026 → 23 Apr 2029. [Download SII certificate](#) · [Download IQNET attestation](#).
- **SOC 2 Type II** — Audit engagement signed; observation period in flight. [Download letter of intent](#). The final SOC 2 Type II report will be available under MNDA on completion.
- **ISO/IEC 42001:2023** — Under internal evaluation.
- **ISO/IEC 27018:2019** — Under internal evaluation.

2. Architecture

Heyou runs on Google Cloud Platform using a managed-services architecture. Customer Data is logically isolated at the application, database, and object-storage layer at the tenant organization level. User Data connected from personal resources is further isolated at the User level within a tenant, scoped by user ID such that Customer admins and other Authorized Users cannot retrieve it unless the connecting User has affirmatively shared specific data with the organization.

User Data is protected by the same encryption, tenant-scoping, and access controls described in this Security Overview. The architectural distinction is scope of access — User-only versus tenant-wide — not a separate security stack.

Data Residency

Customers can be configured for region-aligned deployment. For EU tenants, Customer Data is stored in Google Cloud's europe-north1 region in Finland unless otherwise agreed. US regional deployment may be available where applicable. AI processing through Vertex AI / Gemini is configured to align with the customer's tenant region where supported by the provider, model, and endpoint configuration.

Browser Extension Posture

The Heyou Browser Extension is the surface most CISOs scrutinize first. The platform is engineered so Heyou's backend has no token, no credential, and no privileged path to act against any user's third-party accounts — and so customer administrators retain full enterprise control over what gets installed and how.

In short: Heyou never receives, stores, or replays a token capable of reading, posting, or taking action on a user's behalf against a user's own third-party account. All read operations occur inside the user's authenticated browser session via the extension.

The extension is Manifest V3, distributed exclusively through the Chrome Web Store under a stable extension ID, and deployable via standard Chrome enterprise policies (ExtensionInstallForcelist, ExtensionSettings for version pinning, ExtensionInstallBlocklist) through Microsoft Intune, Jamf, Google Workspace, JumpCloud, or any MDM that pushes Chrome policy.

CRM Connections

Business systems a Customer connects at the organizational level are distinct from the above. Where a Customer connects a CRM such as Salesforce or HubSpot, the connection uses a Customer-provisioned integration user with a permission set the Customer installs and controls. The credential is held server-side, encrypted at rest, and used only for that synchronization. It is not a user credential and does not act on any individual user's behalf.

That permission set is read-only on the standard CRM objects Heyou reads, grants write access only to Heyou's own namespace, and carries **no delete rights on any object**. Heyou's own records live in a dedicated namespace that the Customer can uninstall in one step, removing exactly those records and nothing else. The connection gives Heyou no path into a user's calendar, email, or professional network accounts, and Customer admins can disconnect it at any time, which deletes the corresponding CRM data Heyou holds.

Heyou's Salesforce connected app implements PKCE and refresh-token rotation in line with Salesforce's connected-app security requirements. Tokens are encrypted at rest, no credential is held in source or build configuration, and a rejected or expired token pauses the connection and raises an alert rather than retrying against the Customer's org.

Heyou operates against a configurable per-tenant daily API-call ceiling so the connection cannot exhaust a Customer's org limits, and backs off rather than retrying aggressively when a limit is reached. Call volume is visible to Customer admins. When an admin disconnects the CRM, Heyou deletes the CRM data it holds for that tenant as part of the disconnect operation rather than on a later schedule.

The full posture — per-permission table with justifications, egress allowlist, publisher-account controls, ownership-transfer commitments, and revocation flow — is documented in the [Public Trust Overview, §14 Browser Extension Security Posture](#).

3. Encryption and PII Protection

- At rest: customer data stores and backups are encrypted using Google-managed encryption or equivalent managed cloud encryption.
- In transit: TLS is used on network paths.
- Secrets: managed through Google Secret Manager; secrets are not stored in source code or build logs.
- PII minimization: where direct identifiers are not required for third-party generative AI processing, identifiers such as names, email addresses, and phone numbers may be masked with placeholders before model calls, then re-associated inside Heyou.

4. Access Control

- SSO support via standard enterprise identity protocols.
- MFA enforced for internal administrators.
- Role-based access controls in-product.
- Audit logs available for relevant administrative and security events.
- Production access is limited to approved operational needs and governed by least-privilege principles.
- Access reviews and prompt revocation processes are maintained.

5. Software Development Lifecycle

- Code review required for production changes.
- Branch protection for production branches.
- Static analysis, dependency scanning, and secrets scanning in CI.
- Vulnerability scanning of applications and infrastructure.
- Dependency patching based on severity.
- Change management with rollback procedures.

6. Vulnerability Management

- Continuous scanning of infrastructure and applications.
- Coordinated vulnerability disclosure via dpo@heyoudotio.
- Good-faith vulnerability reports are welcomed and handled under Heyou's coordinated disclosure process.
- Third-party penetration testing and remediation tracking are performed as part of the security program.

7. Monitoring and Incident Response

- 24/7 on-call coverage.
- Documented incident-response runbooks.
- Centralized security and audit logs.
- Post-incident review process.
- Customer notification for confirmed material security incidents involving Customer Data in accordance with the DPA.

8. Business Continuity and Disaster Recovery

- Encrypted backups.
- Recovery processes aligned with service availability objectives.

- Disaster-recovery and crisis-response procedures.
- Testing and tabletop exercises as appropriate to the maturity of the program.

9. People

- Confidentiality agreements for personnel.
- Security and privacy training.
- Role-based training for functions with elevated access.
- Secure device-management practices, including disk encryption and patching.

10. Vendor Management

- Risk-tiered vendor assessment before onboarding.
- Contractual controls including DPA, security addendum where applicable, and confidentiality commitments.
- Re-review for critical vendors.
- Subprocessor change notification in accordance with the DPA.