# Higher Education Community Vendor Assessment Toolkit (HECVAT) 4 — Full

37signals — Basecamp

Completed against the EDUCAUSE HECVAT 4 Full workbook, version 4.1.6

## Contents

**Organization:** 37signals, LLC

**Product in scope:** Basecamp — multi-tenant SaaS operated on 37signals-owned hardware in leased colocation facilities: primary datacenters in Chicago and Ashburn plus a read-only replica in San Jose, all in the United States. Basecamp has no EU datacenter.

**Framework:** the EDUCAUSE Higher Education Community Vendor Assessment Toolkit, HECVAT 4 Full — 331 vendor-facing question IDs across eight sections. The answers were drafted against a version 4.1.0 workbook and reconciled to version 4.1.6 (May 2026), the current release; no question IDs were added or removed anywhere in HECVAT 4.x, so the answer set applies to both. HECVAT is published by EDUCAUSE (CC BY-NC-SA 4.0).

**Report date:** September 2026 (workbook Date Completed: 2026-09-01). Reviewed at least annually or upon significant change.

**Contact:** security@37signals.com

**Formats:** this document is also published as **a PDF**, **a CSV of the full answer set**, and **the filled official EDUCAUSE workbook** (v4.1.6, with formulas, dropdowns, and institution-side scoring sheets intact).

**How to read this document:** each row carries the workbook question, our **Response** (Yes / No / N/A, or a short value for identity fields), and **Additional Information**. A blank Response with a note marks a row answered by explanation rather than a dropdown value — internal operational detail available under NDA, or a row the workbook itself gates off. The GNRL identity rows repeat on every workbook tab and auto-populate from START HERE; they appear once below. Where 37signals does not perform or document a control, the response is an honest **No** and is not represented otherwise.

**Assurance posture:** 37signals, LLC has not completed a company-level SOC 2 or ISO 27001 audit. Independent assurance that does exist is stated where relevant: the colocation provider (Summit, formerly Deft) issues a SOC 2 Type II covering datacenter physical and environmental controls at the Chicago and Ashburn facilities (available under NDA); 37signals runs third-party penetration tests and a public HackerOne bug-bounty program; and it self-assesses PCI DSS SAQ A. This questionnaire is a self-assessment of 37signals' stated posture, not an audited attestation.

## Responses by section

### START HERE

| # | Question | Response | Additional information |
|---|---|---|---|
| GNRL-01 | Solution Provider Name | 37signals LLC | 37signals LLC is the contracting entity named in the DPA. |
| GNRL-02 | Solution Name | Basecamp | The current marketed version is Basecamp 5. Some internal telemetry and status naming still says “Basecamp 4” in places; this is a naming-lag artifact, not two live products. |
| GNRL-03 | Solution Description | Refreshingly simple project management. | |
| GNRL-04 | Solution Provider Contact Name | Chase Clemons | |
| GNRL-05 | Solution Provider Contact Title | Head of Support | |
| GNRL-06 | Solution Provider Contact Email | support@basecamp.com | |
| GNRL-07 | Solution Provider Contact Phone Number | Provided to institutions on request via support@basecamp.com | |
| GNRL-08 | Country of Company Headquarters | USA | 37signals’ registered address, per the Privacy Policy, is in Oak Park, Illinois, USA. |
| GNRL-09 | Employee Work Locations (all) | Remote | 37signals is a fully remote company with no physical headquarters; employees are spread across dozens of cities on multiple continents. |
| COMP-01 | Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?* | Yes | 37signals organizes work into small, dedicated functional teams — Product/Programming, Design, Support, Operations, QA, and Security/Infrastructure/Performance — working in fixed six-week cycles with defined ownership of scope, as described publicly in Shape Up and the Security Overview. |
| COMP-02 | Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships. | Privately held, founder-led LLC | 37signals LLC is a privately held, founder-led limited liability company — not a legal partnership. It has no parent company and no majority-owned subsidiaries; all product lines (Basecamp, HEY, Highrise, Campfire, Backpack) are operated directly by 37signals LLC. There are no institutional investors and no board; the company has taken one minority outside investment (Bezos Expeditions, since 2006). All operations are US-based with a fully distributed, remote workforce; there is no offshoring or multinational subsidiary arrangement. |

| # | Question | Response | Additional information |
|---|---|---|---|
| COMP-03 | Have you operated without unplanned disruptions to this solution in the past 12 months? | No | 37signals maintains a public real-time status page with historical incident and uptime data. The full trailing-12-month incident export (2025-08-26 through 2026-08-26) records 19 posted incidents, every one resolved the same day, none involving data loss. Trailing-12-month uptime is 99.99%+ on every 37signals product, with Basecamp 5 at 99.995%. Full incident history is available on the status page. |
| COMP-04 | Do you have a dedicated information security staff or office? | Yes | 37signals' Operations team and dedicated Security, Infrastructure and Performance (SIP) team own access and identity management, network security, incident response, and coordination of the HackerOne bug bounty program and third-party penetration tests and security reviews, as described in the Security Overview. |
| COMP-05 | Use this area to share information about your environment that will assist those who are assessing your company's data security program. | See the Security Overview | The Security Overview whitepaper covers personnel controls, penetration testing, PCI compliance (SAQ A), encryption in transit, at rest, and at work, physical security, incident management, and data deletion timelines. |
| REQU-01 | Are you offering a cloud-based product? | Yes | Basecamp is a self-serve, multi-tenant SaaS product and platform, not a professional service. The Product and Infrastructure sections of this assessment are completed in full. |
| REQU-02 | Does your product or service have an interface? | Yes | Web, desktop, and mobile app interfaces. |
| REQU-03 | Are you providing consulting services? | No | Basecamp is a self-serve SaaS product; 37signals does not sell implementation or consulting services as part of this offering. |
| REQU-04 | Does your solution have AI features, or are there plans to implement AI features in the next 12 months? | No | Basecamp does not include an AI assistant or AI features of any kind, and 37signals does not use AI with customer data; were that to change, it would be disclosed in the Privacy Policy. Disclosed alongside the No so it is not read as a denial: Basecamp supports Bring-Your-Own-Agent (BYOA) — a customer may connect their own AI agent to their own account through the Basecamp CLI and MCP servers, under the customer's own credentials and the customer's own AI provider's terms; 37signals runs no models on customer content. The Anthropic and OpenAI entries on the Basecamp subprocessor list cover staff use of those tools in day-to-day work (coding, QA, etc.) as part of operating Basecamp; the list covers all processing 37signals may perform in operating the Service and does not imply in-product AI. These details are also disclosed in the AI section of this assessment. |

| # | Question | Response | Additional information |
|---|---|---|---|
| REQU-05 | Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)? | No | Basecamp is a general-purpose project management tool; it is not designed or marketed for processing protected health information, and 37signals does not enter into Business Associate Agreements for it. Customers are responsible for not uploading PHI to the Service. |
| REQU-06 | Is the solution designed to process, store, or transmit credit card information? | No | Credit card data is submitted directly to 37signals' payment processor (Braintree) and does not touch 37signals servers. 37signals stores only the last 4 digits of the card number for invoicing and account history, plus the billing address for tax and fraud detection; it does not store, process, or transmit full cardholder data. 37signals submits a PCI self-assessment (SAQ A), as noted in the Security Overview. |
| REQU-07 | Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment? | No | Basecamp is delivered entirely as multi-tenant SaaS over HTTPS; no on-premises component and no inbound firewall exceptions are required. |
| REQU-08 | Does your solution have access to personal or institutional data? | Yes | 37signals processes customer content and personal data to provide the Service, with narrow, permission-gated staff access. Per the Privacy Policy, no 37signals human looks at customer content except for limited purposes with the customer's express permission. |

## Organization

| # | Question | Response | Additional information |
|---|---|---|---|
| DOCU-01 | Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?* | No | The question is conjunctive — a documented BCP with a clear owner, tested annually — and the testing limb currently fails. The Business Continuity & Operational Resilience Policy (+ BCP) (P-03, adopted 2026-08-31, reviewed at least annually or upon significant change) is documented and owned by the Operations and SIP teams, and documented disaster-recovery practices stand — hourly database backups and off-site backup storage — but recovery drills across diverse failure and disaster scenarios were practiced regularly through early 2024 and have lapsed since (internally attested 2026-09-01; restart pending), and no at-least-annual test attestation exists. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DOCU-02 | Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?* | No | The question is conjunctive — a documented DRP with a clear owner AND annual testing — and the testing limb currently fails: recovery drills across diverse failure scenarios ran regularly through early 2024 and have lapsed since (internally attested 2026-09-01; restart pending). The documented DR capability stands, owned by the Operations and SIP teams under the Business Continuity & Operational Resilience Policy (P-03, adopted 2026-08-31, reviewed at least annually or upon significant change): hourly database backups, automatic file backups on upload, and off-site backup storage. The answer returns to Yes when annual testing resumes. |
| DOCU-03 | Have you undergone a SSAE 18/SOC 2 audit? | No | 37signals LLC has not completed a SOC 2 (SSAE 18) audit and has no current plans to pursue one. SOC reports for the third-party data-center facilities used are available under NDA. See the Security Overview. |
| DOCU-04 | Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)? | No | 37signals does not attest conformance to NIST CSF, CIS Controls, or ISO 27001. Code and infrastructure changes are reviewed against security best practices including OWASP guidance, which is not a formal framework certification. See the Security Overview. |
| DOCU-05 | Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system? | No | 37signals does not publish system or application architecture diagrams. Institutions needing this level of detail can contact security@37signals.com to discuss availability under NDA. |
| DOCU-06 | Does your organization have a data privacy policy? | Yes | A published Privacy Policy covers data collection, use, retention, subprocessors, and data-subject rights; the DPA references it directly. |
| DOCU-07 | Do you have a documented, and currently implemented, employee onboarding and offboarding policy? | Yes | New workers sign confidentiality agreements before receiving access to code or customer data, and VPN/system access is limited to those who need it. On departure, company-managed devices are remotely wiped via MDM (Kandji). See the Security Overview. |
| THRD-01 | Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?* | No | There is no formal, documented third-party security-assessment program prior to onboarding subprocessors. All subprocessors are bound by written data-processing agreements requiring protections no less protective than 37signals' own DPA. |

| # | Question | Response | Additional information |
|---|---|---|---|
| THRD-02 | Do you have contractual language in place with third parties governing access to institutional data?* | Yes | Under the DPA, 37signals contractually requires every subprocessor to sign a written agreement with data-protection obligations at least as protective as 37signals' own DPA, including confidentiality, security, and access-limitation terms. This is a flow-down assurance to customers rather than a document the requesting institution can inspect directly — the underlying subprocessor contracts are private; summarized or certified copies are available on request per the DPA. |
| THRD-03 | Do the contracts in place with these third parties address liability in the event of a data breach?* | No | The customer-facing DPA's liability terms govern 37signals' own liability to the customer, not the terms of private subprocessor agreements. Subprocessor-contract liability language is not publicly published. |
| THRD-04 | Do you have an implemented third-party management strategy?* | Yes | Governed by the Supply Chain / Subprocessor Risk Management Policy (P-12, adopted 2026-08-31, reviewed at least annually or upon significant change): subprocessors are bound by DPA flow-down terms no less protective than 37signals' own DPA, the subprocessor list is published per product, and customers receive advance notice of subprocessor changes with a 10-business-day objection window and may subscribe to change notifications. No formal vendor-tiering scheme is published. |
| THRD-05 | Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)? | No | 37signals is a SaaS provider that does not manufacture or assemble hardware; it owns and operates its own production servers in leased colocation facilities (Summit, formerly Deft). Employee devices are centrally managed via Kandji MDM, but no formal hardware supply-chain or export-licensing procedure is published. |
| CHNG-01 | Will the institution be notified of major changes to your environment that could impact the institution's security posture?* | No | There is no proactive-notification commitment for general infrastructure or environmental changes. The published notification commitment covers new subprocessors: customers are notified before a new subprocessor is authorized and may object within 10 business days, per the DPA. |
| CHNG-02 | Does the system support client customizations from one release to another?* | N/A | Basecamp is a single, standardized multi-tenant SaaS product, not per-customer-forked or on-premises. Account-level configuration is retained automatically across the continuous release process; there is no customer-specific code customization to lose. |

| # | Question | Response | Additional information |
|---|---|---|---|
| CHNG-03 | Do you have an implemented system configuration management process (e.g., secure “gold” images, etc.)?* | Yes | Production systems are provisioned and configured through automated configuration-management tooling to a standard secure configuration expressed as version-controlled code, with changes to that baseline passing through the peer-reviewed change pipeline (Change & Configuration Management Policy P-04 and the Change-Management & Hardening-Baseline Policy, adopted 2026-08-31). The baseline contents are held internal and available to assessors under NDA. Employee workstations run a Kandji-applied standard configuration audited daily by Shipshape. |
| CHNG-04 | Do you have a documented change management process? | Yes | The Change & Configuration Management Policy (P-04, adopted 2026-08-31, reviewed at least annually or upon significant change) documents the process: every change is version-controlled and peer-reviewed by the Operations and SIP teams before merge, automated test suites and static analysis gate merges in CI, changes can be validated on staging/beta, and production releases health-check before traffic cutover, with inherent rollback. |
| CHNG-05 | Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production? | No | No published document describes a formal, staged change-management process for institutional review; changes are reviewed by dedicated internal teams before release. |
| CHNG-06 | Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change? | No | No published documentation confirms a formal dependency-currency check as part of the change process. |
| CHNG-07 | Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications? | Yes | Software infrastructure is updated regularly with the latest security patches, as a standing operational practice. See the Security Overview. |
| CHNG-08 | Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied? | No | 37signals operates automated systems that detect and block suspicious activity as an ongoing compensating control, but no published procedure specifically addresses interim risk mitigation between vulnerability discovery and patch deployment. |

| # | Question | Response | Additional information |
|---|---|---|---|
| CHNG-09 | Do clients have the option to not participate in or postpone an upgrade to a new release? | No | Basecamp is continuously updated, multi-tenant SaaS; customers on the current product cannot opt out of or postpone platform updates. 37signals has historically kept older product generations (Basecamp Classic, 2, and 3) running indefinitely for customers who never migrated, but transitions within the currently assessed product are mandatory. |
| CHNG-10 | Do you have a fully implemented solution support strategy that defines how many concurrent versions you support? | No | Partial: 37signals has a long-standing informal practice of keeping legacy product generations (Basecamp Classic, 2, and 3) running indefinitely for customers who never migrated, rather than forcing end-of-life. No formal policy defining a number of concurrently supported versions, and no customer-distribution percentages, are published. |
| CHNG-11 | Do you have a release schedule for product updates? | No | No fixed release schedule or calendar is published; Basecamp ships continuously via rolling updates, with features announced on the company dev blog as they ship. |
| CHNG-12 | Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed? | No | No, by design: 37signals' published product methodology, Shape Up, explicitly rejects long-range roadmaps. Work is planned six weeks at a time via a betting table rather than a maintained backlog. |
| CHNG-13 | Can solution updates be completed without institutional involvement (i.e., technically or organizationally)? | Yes | Basecamp is hosted SaaS with no client-side software to install or maintain. Deployments use Kamal, 37signals' own open-source zero-downtime deployment tool, built and used to run its product line; Kamal performs zero-downtime deploys with health-checked cutover, so releases require no maintenance window. |
| CHNG-14 | Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer? | Yes | Releases use the Kamal zero-downtime deployment mechanism: a new version is booted and health-checked before traffic is switched over, so releases require no maintenance window and produce no customer-visible downtime. |
| CHNG-15 | Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)? | No | No published documentation describes a formal emergency-change procedure with after-the-fact authorization. |

| # | Question | Response | Additional information |
|---|---|---|---|
| CHNG-16 | Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)? | No | Company-owned Mac computers are centrally managed via Kandji MDM (standard configuration, disk encryption, firewall, password rules, remote wipe) and continuously audited via Shipshape. No equivalent, comprehensive strategy covering appliances, cloud-service configuration, or employee-owned (BYOD) devices is published. See the Security Overview. |
| PPPR-01 | Do you have a documented patch management process?* | Yes | Software infrastructure is updated regularly with the latest security patches. See the Security Overview. |
| PPPR-02 | Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?* | No | Privacy and security policies are set at the customer-wide level, not per institution; no customization to an individual institution's internal IT policy requirements is offered. |
| PPPR-03 | Is your company subject to the institution's geographic region's laws and regulations? * | No | 37signals LLC is a U.S. company headquartered in Oak Park, Illinois. It is subject to applicable U.S. federal and Illinois state law and, where contractually agreed via the DPA, EU/UK/Swiss and U.S. state privacy laws — not separately to the requesting institution's specific state or regional laws. |
| PPPR-04 | Can you accommodate encryption requirements using open standards? | Yes | TLS with AES-128-CBC, SHA-2, and ECDHE-RSA protects data in transit; files at rest are encrypted with AES-256 with SHA-256 for integrity; passwords are hashed with BCrypt; backups are encrypted with GPG. See the Security Overview. |
| PPPR-05 | Do you have a documented systems development life cycle (SDLC)? | Yes | 37signals publicly documents its product development methodology, Shape Up (six-week shaping/betting/building cycles, hill-chart progress tracking, cool-down periods), which is the process used to build and ship Basecamp itself. Shape Up governs product-development cadence and planning; it does not itself specify security gates. Security review of code and infrastructure changes is a separate, parallel practice rather than a named stage within Shape Up. |
| PPPR-06 | Do you perform background screenings or multi-state background checks on all employees prior to their first day of work? | No | Background checks are not performed on employees or contractors. See the Security Overview. |

| # | Question | Response | Additional information |
|---|---|---|---|
| PPPR-07 | Do you require new employees to fill out agreements and review policies? | Yes | All new employees and contractors sign confidentiality agreements before receiving access to code and customer data; the obligations survive termination. See the Security Overview and DPA. |
| PPPR-08 | Do you have a documented information security policy? | Yes | Security practices are documented in the published Security Overview, which the DPA formally incorporates by reference as the Security, Privacy and Architecture Documentation governing 37signals' technical and organizational measures. This is an externally facing document rather than an internal ISMS policy with version history; if a review requires the latter specifically, security@37signals.com can discuss additional internal documentation shareable under NDA. |
| PPPR-09 | Are information security principles designed into the product lifecycle? | Yes | Code and infrastructure changes are reviewed for security best practices, including OWASP guidance, before release. Newer applications including Basecamp use field-level "encryption at-work," where each database field is individually encrypted so engineers can operate and support the product without being exposed to customer content. See the Security Overview. |
| PPPR-10 | Will you comply with applicable breach notification laws? | Yes | 37signals commits contractually (DPA) to notify customers without undue delay, and in compliance with applicable data protection law, after becoming aware of a Personal Data Incident. Separately, the Security Overview — which the DPA incorporates by reference — commits to contacting the account owner within 24 hours of an incident and working with the customer throughout. |
| PPPR-11 | Do you have an information security awareness program? | Yes | Everyone at 37signals is trained and made aware of security concerns and best practices relevant to their systems and role. See the Security Overview. |
| PPPR-12 | Is security awareness training mandatory for all employees? | Yes | Published materials describe this as a universal practice (everybody is trained) rather than using the specific word "mandatory"; completion-tracking and attestation records for this training are not published. See the Security Overview. |
| PPPR-13 | Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts? | No | The recurring documented control is the bi-weekly audit of employee access to customer data (console1984 and audits1984, per the Security Overview), which reviews access events rather than the membership or entitlements of privileged accounts; a documented procedure specifically reviewing and updating privileged-account access lists is not attested — the published CAIQ rates access revalidation Partial for this reason. Admin access is limited need-to-know over VPN with 2FA. |
| PPPR-14 | Do you have documented, and currently implemented, internal audit processes and procedures? | Yes | Scoped: a documented, recurring internal audit of employee access to customer data runs bi-weekly using console1984 and audits1984. 37signals does not maintain a broader enterprise internal-audit function (financial/operational); it is a privately held company without a dedicated internal-audit department. |

| # | Question | Response | Additional information |
|---|---|---|---|
| PPPR-15 | Does your organization have physical security controls and policies in place? | Yes | 37signals is a fully remote company with no corporate office housing customer data. Production infrastructure runs in third-party data centers with biometric access locks, round-the-clock interior and exterior surveillance, and 24/7/365 onsite staff; only authorized personnel have access. See the Security Overview. |

## Product

| # | Question | Response | Additional information |
|---|---|---|---|
| AAAI-01 | Does your solution support single sign-on (SSO) protocols for user and administrator authentication?* | No | Basecamp does not support SSO or SAML-based single sign-on. Users authenticate with an email address and password, or by signing in with a Google account. |
| AAAI-02 | For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?* | Yes | All Basecamp authentication is local: email/password, or Sign in with Google. Since Basecamp has no SSO/SAML option, local authentication is the method available to every customer. |
| AAAI-03 | For customers not using SSO, can you enforce password/ passphrase complexity requirements (provided by the institution)?* | No | There is no mechanism for a customer to impose its own password policy; Basecamp enforces one fixed, vendor-defined policy for all accounts, consistent with the absence of SSO and directory integration. |
| AAAI-04 | For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?* | Yes | Passwords must be at least 12 characters, must not match the username/email, and must not appear in known-breach corpora (screened against Have I Been Pwned via a k-anonymity range query). There is no character-composition requirement (no mandated numbers or symbols); strength rests on length plus breach screening. Passwords are stored BCrypt-hashed. |
| AAAI-05 | For customers not using SSO, do you have documented password/ passphrase reset procedures that are currently implemented in the system and/or customer support?* | Yes | Self-service password reset via emailed link; account owners and admins can trigger a reset email for any team member from Adminland. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AAAI-06 | Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?* | No | Follows directly from Basecamp having no SAML/SSO support. |
| AAAI-07 | Are there any passwords/ passphrases hard-coded into your systems or solutions? * | No | No passwords or passphrases are hard-coded into systems or solutions. |
| AAAI-08 | Are you storing any passwords in plaintext?* | No | All passwords are hashed and salted using BCrypt (cost factor 10); plaintext passwords are never stored, as documented in the Security Overview. |
| AAAI-09 | Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?* | Yes | Audit logs covering all four elements exist and are held by 37signals: login events are logged with IP address, browser, OS, and timestamp — surfaced to users, with new-device email notification and per-user login history; 37signals logs all access to all accounts by IP address; and centralized off-host server-side request logging records in-app actions performed with source IP, used by the Security team for its own operations. In-app activity timelines additionally record actions performed per person. There is no single customer-admin-facing, account-wide view combining these — the combined logs are vendor-held, with the per-user login history as the customer-visible slice. |
| AAAI-10 | Describe or provide a reference to the (a) system capability to log security/ authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.* | Internally logged; not customer-exposed | 37signals internally logs account access by IP address and audits internal employee access to customer data bi-weekly (console1984/audits1984 tooling), as described in the Security Overview. No customer-facing SIEM or log-collector integration is published or offered to customers. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AAAI-11 | Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?* | Yes | Documentation is available to assessors under NDA: central security/infrastructure logs are retained 30 days (retention enforced by the log platform), and privileged-console session records for Basecamp are incinerated after 30 days; log management is restricted to the Operations and SIP teams. These logs are internal and not accessible to customers. |
| AAAI-12 | For customers not using SSO, does your application support integration with other authentication and authorization systems? | No | Basecamp has no SSO, SAML, or directory-integration support; no integration with external authentication or authorization systems is available. |
| AAAI-13 | Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ ePPN/ePE) | No | Not applicable in practice: no SSO/SAML integration exists to configure attribute mappings against. |
| AAAI-14 | For customers not using SSO, does your application support directory integration for user accounts? | No | No LDAP, Active Directory, SCIM, or other directory-integration feature; accounts are created and managed manually inside Basecamp by owners and admins. |
| AAAI-15 | Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other? | No | Basecamp supports none of these web SSO standards. Sign in with Google is a consumer convenience login (OAuth against the user's personal Google account), not an institution-controlled OIDC/SSO integration, and does not satisfy this requirement. |
| AAAI-16 | Do you support differentiation between email address and user identifier? | No | A user's Basecamp login is their email address; no separate customer-facing or institution-configurable user identifier exists. Internally, 37signals maintains a single cross-product 37signals ID per person spanning multiple accounts, but it is not institution-visible or configurable. |
| AAAI-17 | For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)? | Yes | Native two-factor authentication: a TOTP code from an authenticator app, with an option to add a hardware security key (USB key, fingerprint reader, Windows Hello). Account owners can require 2FA for all members from Adminland; admins can deactivate a locked-out member's 2FA on their behalf. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AAAI-18 | Does your application automatically lock the session or log out an account after a period of inactivity? | No | No automatic inactivity timeout or session lock. Sessions persist via a browser cookie until manual logout (which signs out of all Basecamp accounts on that device) or until cookies are cleared. |
| DATA-01 | Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?* | | Not publicly documented. Based on standard SaaS architecture, database and file storage servers would not be expected on publicly routable IPs — only edge/web-facing infrastructure — but this is not confirmed in published documentation. |
| DATA-02 | Is the transport of sensitive data encrypted using security protocols/ algorithms (e.g., system-to-client)?* | Yes | Transport is encrypted with TLS 1.2/1.3 using ECDHE key exchange; modern clients negotiate TLS 1.3 with AES-256-GCM, and AEAD cipher suites are preferred (publicly verifiable via SSL Labs). A legacy TLS 1.2 CBC fallback (ECDHE-RSA-AES128-SHA256) remains negotiable for older clients. The transport-cipher description in the published Security Overview (GeoTrust/RapidSSL certificates, AES_128_CBC) predates the current configuration; the published CAIQ (CEK-03.1) records the current state. |
| DATA-03 | Is the storage of sensitive data encrypted using security protocols/ algorithms (e.g., disk encryption, at-rest, files, and within a running database)?* | Yes | Uploaded files are encrypted at rest using AES-256; backups are encrypted using GPG. Application databases are not encrypted at rest in the traditional disk-encryption sense; for Basecamp 5, 37signals instead uses field-level "encryption at-work" — every content field is encrypted with its own key, itself encrypted with a master key — so data stays encrypted while the database is actively serving requests. Passwords are hashed and salted with BCrypt and never stored recoverably. Note: the Security Overview states at-work encryption applies to HEY and Basecamp 5, while the Privacy Policy names HEY specifically; the Security Overview, as the more specific purpose-built document, is relied on here. |
| DATA-04 | Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?* | No | No published claim of FIPS-validated cryptographic modules. |
| DATA-05 | Will the institution's data be available within the system for a period of time at the completion of this contract?* | Yes | Content becomes inaccessible via the live application immediately upon cancellation but is not immediately destroyed: contacting support can restore access within the first 30 days after cancellation. After 30 days, content is permanently deleted from active systems; backup copies are purged within 60 days, per the Terms of Service. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DATA-06 | Are ownership rights to all data, inputs, outputs, and metadata retained even through a provider acquisition or bankruptcy event? * | No | No contractual guarantee is published; the standard Terms of Service do not address acquisition- or bankruptcy-specific data rights. |
| DATA-07 | Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?* | Yes | Primary data centers are in Chicago, IL and Ashburn, VA; Basecamp 5 also maintains a read-only outpost in San Jose, CA — all US locations. (HEY separately maintains an Amsterdam, Netherlands outpost; that does not apply to Basecamp.) |
| DATA-08 | Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?* | Yes | Data centers are physically secured with biometric locks, round-the-clock surveillance, restricted access, and 24/7/365 onsite staff. |
| DATA-09 | At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives? | Yes | Customers can export a full copy of their data before cancellation. After cancellation, content is permanently deleted from active systems within 30 days and from backups within 60 days; 37signals states it cannot recover data once permanently deleted. |
| DATA-10 | Can the institution extract a full or partial backup of data? | Yes | Account owners can export a full HTML copy of Basecamp data at any time — the entire account, a selection, or individual projects, including archived projects and Ping conversations. There is no native CSV or JSON export; the HTML export is designed for local viewing and backup rather than migration. Only account owners can access this feature. |
| DATA-11 | Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery? | Yes | Hourly database backups and automatic file backups; disaster-recovery drills covering diverse disaster/failure scenarios were practiced regularly through early 2024 and have lapsed since (internally attested 2026-09-01; restart pending). Published material itemizes database and uploaded-file backups plus restoration testing; it does not separately itemize operating-system, utility, or security-software backup contents — recovery of those layers was exercised through the drills rather than evidenced as a backup-content inventory. |
| DATA-12 | Are you performing off-site backups (i.e., digitally moved off site)? | Yes | Backups are stored off-site for a maximum of 30 days. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DATA-13 | Are physical backups taken off-site (i.e., physically moved off site)? | N/A | No physical backup media exist to move: the published backup process is digital, network-based off-site storage of GPG-encrypted backups across redundant data centers, with no physical media transported off-site. On pre-4.1.5 workbooks, whose dropdown offers only Yes/No on this row, the answer is No — the position is identical. |
| DATA-14 | Are data backups encrypted? | Yes | Backups of customer data are encrypted using GPG. |
| DATA-15 | Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures? | Yes, scoped | The Media Sanitization & Secure-Disposal Standard (adopted 2026-08-31, reviewed annually and on significant change) requires that storage media that held customer or personal data be sanitized or physically destroyed per NIST SP 800-88 before disposal, reuse, or return, with the same requirement flowing down to the colocation provider; managed staff devices are remote-wiped on loss or decommission. The standalone written operational procedure and records mechanism are provisional pending internal operational confirmation. |
| DATA-16 | Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards? | Yes | The Media Sanitization & Secure-Disposal Standard specifies NIST SP 800-88 (purge/clear methods that render recovery infeasible, or physical destruction). DoD 5220.22-M is not referenced. The specific technique per media type and the sanitization records are held internally, available under NDA. |
| DATA-17 | Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means? | Yes | Staff can access customer data for support purposes only with the customer's express consent requested in advance; staff do not access data as a matter of course. Field-level encryption at-work (Basecamp 5) limits what engineers and admins can see during internal operations, and all employee access is audited bi-weekly (console1984/audits1984). See DATA-03 for the note on the documented scope of at-work encryption. |
| DATA-18 | Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)? | Yes | Employee Mac computers are centrally managed via Kandji (disk encryption, firewall, password rules, app updates, remote wipe). VPN with two-factor authentication is required for internal server access. All computers are hardened and audited daily via Shipshape. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DATA-19 | Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy). | No | No dedicated single-tenant deployment option is available; Basecamp is offered exclusively as multi-tenant SaaS. Each customer's data lives in its own logically scoped account within shared application and database infrastructure. |
| DATA-20 | Are ownership rights to all data, inputs, outputs, and metadata retained by the institution? | Yes | All materials submitted to the service remain the customer's property; 37signals is granted only a limited license to use submitted content to operate the service, per the Terms of Service. |
| DATA-21 | In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications? | No | No published commitment to a specific notice period exists in the standard Terms of Service or Privacy Policy. |
| DATA-22 | Are involatile backup copies made according to predefined schedules and securely stored and protected? | Yes | Database backups run hourly and files are backed up automatically on upload. Backups are encrypted with GPG, tested regularly, and stored off-site for up to 30 days. |
| DATA-23 | Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)? | No | No single documented lifecycle process (generation, exchange, storage, vetting, replacement) covers all system components. Implemented practice: for Basecamp 5, every content field is encrypted with its own key (field-level encryption at-work); backups are GPG-encrypted; TLS certificates and secrets are managed by the Operations and SIP teams under the Cryptography & Key Management Policy (P-05, adopted 2026-08-31). Rotation, custody, and replacement procedures are not yet documented end-to-end; the published CAIQ rates the corresponding controls Partial. |

## Infrastructure

| # | Question | Response | Additional information |
|---|---|---|---|
| APPL-01 | Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?* | Yes | Basecamp account permissions are structured — owner and administrator roles, project-level access, and per-person visibility controls — consistent with role-based access control. |
| APPL-02 | Are you using a web application firewall (WAF)?* | Yes | Production Basecamp web traffic is fronted by Cloudflare with the Cloudflare Managed Ruleset and the OWASP Core Ruleset enabled on the production zones, plus zone rate limiting — a dedicated HTTP/application-layer WAF, distinct from the network-layer firewalls described in the Security Overview. Application-layer protection additionally includes framework-level defenses, an internally built anomaly-detection and auto-blocking system, and continuous external testing through the public HackerOne program. |
| APPL-03 | Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/ application(s) that will have access to institution's data?* | Yes | The software infrastructure is updated regularly with the latest security patches, per the Security Overview. |
| APPL-04 | Does your application require access to location or GPS data? * | No | Basecamp's mobile apps do not request GPS or location access; the Privacy Policy lists the device permissions the apps may request (contacts, calendar, camera, push notifications, file access), and location/GPS is not among them. |
| APPL-05 | Does your application provide separation of duties between security administration, system administration, and standard user functions?* | Yes | Dedicated Operations and SIP (security/infrastructure) teams are in charge of access and identity management, network connectivity, firewalls, and log file management, distinct from application-level user roles. |
| APPL-06 | Do you subject your code to static code analysis and/or static application security testing prior to release?* | Yes | The SIP team is responsible for reviewing all changes to code and infrastructure against best practices and security guidelines, including OWASP. |

| # | Question | Response | Additional information |
|---|---|---|---|
| APPL-07 | Do you have software testing processes (dynamic or static) that are established and followed?* | Yes | Code and infrastructure changes undergo OWASP-aligned review; HEY and Basecamp 5 have also undergone security reviews and penetration tests performed by third-party security firms. |
| APPL-08 | Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC? | Yes | Remote and administrative access to 37signals infrastructure is limited to staff who need it for their day-to-day work and requires two-factor authentication over VPN. |
| APPL-09 | Does the system provide data input validation and error messages? | Yes | As a mature production SaaS application subject to structured testing and static analysis, Basecamp performs data input validation and returns application error messages; this practice is not separately documented in a public statement. |
| APPL-10 | Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)? | Yes | 37signals follows a documented engineering philosophy of minimizing third-party dependencies and manages its Ruby and JavaScript dependency surface through standard tooling; code and infrastructure changes go through team review. |
| APPL-11 | Have your developers been trained in secure coding techniques? | Yes | All 37signals workers are trained and made aware of security concerns and best practices. |
| APPL-12 | Was your application developed using secure coding techniques? | Yes | Development follows OWASP-aligned review practices, static analysis, and third-party penetration testing. |
| APPL-13 | If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)? | Yes | The current Basecamp mobile app (Basecamp — Project Management) is distributed exclusively through the Apple App Store and Google Play Store. |
| APPL-14 | Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application? | Yes | Employee access to customer data in Basecamp is access-controlled and independently audited on a bi-weekly cadence using the console1984 and audits1984 tooling. |
| DCTR-01 | Select your hosting option. | Physical Co-Location | 37signals owns and operates its own server hardware, hosted in leased colocation space at Summit (formerly Deft) facilities in Chicago, IL and Ashburn, VA; neither public cloud, private cloud, nor traditional on-premise. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DCTR-02 | Is a SOC 2 Type 2 report available for the hosting environment? | Yes | For physical and environmental controls: the colocation provider, Summit (formerly Deft), issues an annual SOC 2 Type II report covering the facilities 37signals uses, and the current-cycle report is available from Summit on request. 37signals LLC itself has not completed a SOC audit; application- and organization-layer controls are addressed by 37signals' own published security program. |
| DCTR-03 | Are you generally able to accommodate storing each institution's data within its geographic region? | No | All Basecamp data is stored in 37signals' primary US data centers (Chicago and Ashburn), with a US-based read-only outpost in San Jose, CA for latency; per-institution geographic data placement is not offered. |
| DCTR-04 | Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 × 7 x 365)? | Yes | The data centers have 24/7/365 onsite staff. |
| DCTR-05 | Are your servers separated from other companies via a physical barrier, such as a cage or hard walls? | Yes | 37signals equipment occupies dedicated cabinets; the Ashburn facility documents crash-rated, anti-climb cages with dual-factor biometric and proximity access control. |
| DCTR-06 | Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?* | Yes | Facilities use biometric locks, round-the-clock surveillance, and authorized-personnel-only access; Ashburn cages are crash-rated and anti-climb. Summit's current SOC 2 Type II report, available on request, substantiates the physical controls. |
| DCTR-07 | Are your primary and secondary data centers geographically diverse? | Yes | The facilities are in Ashburn, VA and Chicago, IL — roughly 700 miles apart, in different regions and power grids. |
| DCTR-08 | Is the service hosted in a high-availability environment? | Yes | Basecamp runs active/active across both data centers using BGP Anycast; other critical applications run active/standby with failover capability. |
| DCTR-09 | Is redundant power available for all data centers where institutional data will reside? | Yes | Chicago and Ashburn (the primary sites, Summit): 2N UPS redundancy with generator capacity (150,000 kW Chicago; 12,000 kW Ashburn) and a 100% power-uptime SLA. The San Jose read-only replica site is Summit-managed and sits in a facility on the in-scope subservice-facility list of Summit's SOC 2 Type II report, which attests that each subservice facility is fully equipped with redundant UPS, backup generators, and cooling. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DCTR-10 | Are redundant power strategies tested?* | Yes | Redundant-power testing is attested in Summit's SOC 2 Type II report: generators are tested on an annual basis, third-party preventive maintenance inspections of the generators run annually, and third-party specialists inspect power-management systems on a predefined maintenance schedule, with UPS units covering temporary loss or surge. Summit also publishes a 100% power-uptime SLA for these facilities. |
| DCTR-11 | Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested? | Yes | Cooling is N+1 concurrently maintainable at both Chicago and Ashburn, with SLA commitments. Summit's SOC 2 Type II report attests that fire detection and suppression equipment is in place at each data center, with third-party specialists inspecting those systems on an annual basis. The San Jose read-only replica site (Summit-managed, in an in-scope subservice facility — see DCTR-09) is covered by the report's subservice-organization controls: fire detection and suppression equipment and HVAC systems, with inspection reports retained on at least an annual basis. |
| DCTR-12 | Do you have Internet Service Provider (ISP) redundancy? | Yes | Each data center has external connections to the internet, to the other data center, and to AWS, each using diverse physical paths. |
| DCTR-13 | Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility? | Yes | Chicago (350 E Cermak, one of the most carrier-dense colocation buildings in the US) offers an extensive carrier ecosystem with three diverse fiber paths; Ashburn has two diverse fiber paths and direct links to all major carriers and public cloud providers. |
| DCTR-14 | Do you require multifactor authentication for all administrative accounts in your environment? | Yes | Remote access to servers is via VPN with two-factor authentication, limited to workers who need it for their day-to-day work. |
| DCTR-15 | Are you using your cloud provider's available hardening tools or pre-hardened images? | N/A | 37signals runs its own hardware in colocation facilities rather than a public cloud provider's virtualized environment, so no cloud-provider-supplied hardening toolchain exists in the production stack; 37signals hardens its own images and configuration directly. |
| DCTR-16 | Does your cloud solution provider have access to your encryption keys? | No | 37signals does not use a cloud provider for production infrastructure, and no outside provider holds its encryption keys: keys for stored files and for Basecamp 5 database content are managed internally, not by the colocation provider. |
| FIDP-01 | Are you utilizing a stateful packet inspection (SPI) firewall?* | Yes | Products run on a dedicated network secured with firewalls and carefully monitored, per the Security Overview. |

| # | Question | Response | Additional information |
|---|---|---|---|
| FIDP-02 | Do you have a documented policy for firewall change requests?* | No | No public statement confirms or denies a formal firewall change-request process. |
| FIDP-03 | Have you implemented an intrusion detection system (network-based)?* | Yes | 37signals operates an internally built system that monitors and automatically blocks suspicious network- and application-layer activity, including vulnerability scanning and failed-login patterns; this is a custom in-house system rather than a named commercial IDS product. |
| FIDP-04 | Do you employ host-based intrusion detection?* | No | The intrusion monitoring system operates at the network/application-ingress layer; per-host IDS agents are not described in published material. |
| FIDP-05 | Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?* | | Infrastructure and firewall change-log detail is internal operational detail, available under NDA on request; published logging statements cover account access by IP address. |
| FIDP-06 | Is authority for firewall change approval documented? Please list approver names or titles in Additional Info. | | Firewall change approver identities and titles are internal operational detail, available under NDA on request. |
| FIDP-07 | Have you implemented an intrusion prevention system (network-based)? | Yes | The same internally built system both monitors and automatically blocks suspicious activity, providing prevention as well as detection; it is a custom in-house system rather than a named commercial IPS product. |
| FIDP-08 | Do you employ host-based intrusion prevention? | No | As with host-based detection, the prevention capability operates at the network/application layer; per-host prevention agents are not described in published material. |
| FIDP-09 | Are you employing any next-generation persistent threat (NGPT) monitoring? | | Not addressed in published material; internal operational detail, available under NDA on request. The internally built automated monitoring and blocking system is the closest published capability but is not described as NGPT-class monitoring. |
| FIDP-10 | Is intrusion monitoring performed internally or by a third-party service? | Internal | Intrusion monitoring is performed by 37signals' own internally built system, with alerts escalated to the dedicated Operations/SIP team for manual investigation. |
| FIDP-11 | Do you monitor for intrusions on a 24 × 7 x 365 basis? | Yes | Automated monitoring and blocking run continuously by design, and 37signals commits to contacting affected account owners within 24 hours of an incident; an explicit 24×7×365 human-staffing claim is not separately published. |

| # | Question | Response | Additional information |
|---|---|---|---|
| HFIH-01 | Do you have a formal incident response plan? | Yes | Incident response is governed by the Security Incident Response & Forensics Policy (P-11, adopted 2026-08-31, reviewed at least annually or upon significant change); the SIP and Operations teams review, test, and design incident response processes and respond to security-event alerts, with a published commitment to contact affected account owners within 24 hours of an incident. The published CAIQ (SEF-03.1) rates the corresponding response-plan control Partial: a plan artifact with a full communication strategy, including supply-chain notification, is not separately published. |
| HFIH-02 | Do you either have an internal incident response team or retain an external team? | Yes | Internal: dedicated internal Operations and SIP teams are responsible for incident response — the question is satisfied by an internal team. |
| HFIH-03 | Do you have the capability to respond to incidents on a 24 x 7 × 365 basis? | Yes | 37signals maintains continuous automated monitoring with escalation to the Operations team and commits to contacting affected customers within 24 hours of an incident; an explicit published 24×7×365 staffing commitment is not available. |
| HFIH-04 | Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents? | No | 37signals does not carry cyber-risk insurance. |
| VULN-01 | Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?* | Yes | Consistent with the static application security testing and established testing processes applied prior to release; the authenticated-scanning practice is not separately documented in a public statement. |
| VULN-02 | Will you provide results of application and system vulnerability scans to the institution?* | No | Per-customer sharing of vulnerability scan results is not offered; the public HackerOne bug bounty program is the designated external-facing security testing channel. |
| VULN-03 | Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?* | No | External testing is channeled through the public HackerOne bug bounty program, the designated and controlled channel, rather than ad hoc institutional scanning. |

| # | Question | Response | Additional information |
|---|---|---|---|
| VULN-04 | Have your systems and applications had a third-party security assessment completed in the last year? | Yes | 37signals has undergone third-party security reviews and penetration tests for HEY and Basecamp 5, and has run a continuous public HackerOne bug bounty program since October 2020 as an ongoing external testing channel; a specific date for the most recent formal third-party penetration test is not published. |
| VULN-05 | Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)? | Yes | Static application security testing prior to release plus authenticated vulnerability scanning before new releases, supplemented by continuous crowdsourced testing through the public HackerOne bug bounty program. |
| VULN-06 | Are your systems and applications regularly scanned externally for vulnerabilities? | Yes | Continuously tested by external, independent security researchers through the public HackerOne bug bounty program since October 2020. |

## IT Accessibility

| # | Question | Response | Additional information |
|---|---|---|---|
| ITAC-01 | Solution Provider Accessibility Contact Name | Michael Berger | Michael Berger leads quality and accessibility at Basecamp. |
| ITAC-02 | Solution Provider Accessibility Contact Title | Quality & Accessibility Lead | Per his public self-description, he leads quality and accessibility at Basecamp. |
| ITAC-03 | Solution Provider Accessibility Contact Email | accessibility@basecamp.com | accessibility@basecamp.com is a dedicated accessibility address, distinct from the general support@basecamp.com channel. |
| ITAC-04 | Solution Provider Accessibility Contact Phone Number | N/A | No phone contact is published for accessibility; please use accessibility@basecamp.com. |
| ITAC-05 | Web Link to Accessibility Statement or VPAT | https://basecamp.com/accessibility and https://37signals.com/policies/accessibility | basecamp.com/accessibility is Basecamp's accessibility statement; 37signals.com/policies/accessibility carries the published Basecamp Accessibility Conformance Report (VPAT). See ITAC-06 on the ACR's report date. |
| ITAC-06 | Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?* | No | A formal Basecamp Accessibility Conformance Report (VPAT 2.4Rev International Edition) is published at 37signals.com/policies/accessibility (live 2026-08-31), but the report's own face reads "Report Date: June 2025 (Replaces VPAT 2.4 completed 08/2023)" — outside the trailing 12 months — and names Basecamp 4 as the product and version. Until the ACR is re-reviewed and re-issued with a current report date, the honest answer to "created or updated within the past 12 months" stays No, with the published ACR disclosed alongside it. |

| # | Question | Response | Additional information |
|---|---|---|---|
| ITAC-07 | Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?* | No | 37signals is actively working toward WCAG 2.2 level AA and treats it as the target standard, but does not offer a contractual conformance warranty. |
| ITAC-08 | Does the solution substantially conform to WCAG 2.1 AA?* | No | Qualified: Basecamp is designed and tested against WCAG 2.2 level AA guidelines (a superset of 2.1 AA) as an ongoing practice — new features are built with accessibility in mind, tested for keyboard operability and color contrast, and scanned with automated tooling (axe-core) — but 37signals does not formally attest to full conformance, and the published Basecamp Accessibility Conformance Report (self-assessed, report-dated June 2025) records Partially Supports on several WCAG success criteria (e.g., 2.1.1 Keyboard, 1.4.2 Audio Control) rather than attesting substantial conformance. See 37signals.com/policies/accessibility. |
| ITAC-09 | Do you have a documented and implemented process for reporting and tracking accessibility issues?* | Yes | Accessibility issues can be reported to accessibility@basecamp.com. Automated regression scanning (axe-core) runs in the system test suite, complemented by regular manual audits of shipped features. |
| ITAC-10 | Do you have documentation to support the accessibility features of your solution? | Yes | Published documentation supports the solution's accessibility features: the Basecamp Accessibility Conformance Report (criterion-by-criterion support levels with remarks, covering the web app, the iOS and Android apps, and documentation) at 37signals.com/policies/accessibility, the accessibility statement, and platform-specific assistive-technology guidance (the desktop app; VoiceOver on iOS; TalkBack on Android). No dedicated administrator configuration guide is maintained. |
| ITAC-11 | Has a third-party expert conducted an audit of the most recent version of your solution? | No | The most recent public third-party engagement (Aspiritech, a CPACC/WAS-certified accessibility QA vendor) dates to November 2020 and was scoped to the HEY product at launch, not a recent audit of the current Basecamp version. |
| ITAC-12 | Do you have a documented and implemented process for verifying accessibility conformance? | Yes | Automated axe-core scans run as part of the system test suite to guard against regressions; features are manually tested for keyboard operability and screen-reader compatibility before and after shipping, alongside periodic full-app audits. |

| # | Question | Response | Additional information |
|---|---|---|---|
| ITAC-13 | Have you adopted a technical or legal standard of conformance for the solution? | Yes | The target standard is WCAG 2.2 level AA. |
| ITAC-14 | Can you provide a current, detailed accessibility roadmap with delivery timelines? | No | No accessibility roadmap or delivery timeline is published. |
| ITAC-15 | Do you expect your staff to maintain a current skill set in IT accessibility? | Yes | A named staff member (Michael Berger) leads quality and accessibility, working with product and engineering on accessibility practices, and 37signals has engaged outside accessibility-testing specialists historically. No formal certification (IAAP, Trusted Tester) is claimed for named staff. |
| ITAC-16 | Do you have documented processes and procedures for implementing accessibility into your development lifecycle? | Yes | Accessibility is considered at the design stage of every new feature rather than retrofitted afterward; automated accessibility checks (axe-core) run in the same system test suite that gates every release, and features are manually tested for keyboard and screen-reader support before shipping. |
| ITAC-17 | Can all functions of the application or service be performed using only the keyboard? | Yes | Keyboard operability is a design and test requirement for every feature; the accessibility page states a mouse isn't required to perform any action throughout the app. One disclosed edge: the published Basecamp Accessibility Conformance Report rates WCAG 2.1.1 Keyboard as Partially Supports for the web app — the @mention name picker is the one remaining autocomplete element in need of improvement (as of 08/2023). See 37signals.com/policies/accessibility. |
| ITAC-18 | Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including "overlay" or AI-based alternates) for accessibility purposes? | No | No overlay, lite version, or alternate accessibility mode is used; accessibility is built into the single primary interface rather than provided as a bolt-on mode. |

### Case-Specific

Four Case-Specific sections — Consulting, HIPAA, PCI-DSS, and On-Prem, 60 rows in total — are gated off by the workbook itself based on the START HERE answers (REQU-03, REQU-05, REQU-06, and REQU-07, each an accurate No): every gated row's guidance auto-populates "this question does not apply," and the Answer cells stay blank by design. Per the workbook's own instructions, each

section's first row carries a note in Additional Information stating why, rather than leaving 60 silent blanks:

| Rows | Gated by | Additional information (recorded on the section's first row) |
|---|---|---|
| CONS-01–09 | REQU-03 = No | N/A — gated by REQU-03 (No): Basecamp is a self-serve SaaS product; 37signals does not provide implementation or consulting services with this offering. |
| HIPA-01–29 | REQU-05 = No | N/A — gated by REQU-05 (No): Basecamp is a general-purpose project management tool, not designed or marketed for protected health information; 37signals does not enter into Business Associate Agreements for it, and customers are responsible for not uploading PHI. |
| PCID-01–12 | REQU-06 = No | N/A — gated by REQU-06 (No): cardholder data is submitted directly to the payment processor and does not transit 37signals servers; 37signals stores only the last four digits of the card and the billing address, and files a PCI DSS SAQ A merchant self-assessment (a self-assessment, not a certification). |
| OPEM-01–10 | REQU-07 = No | N/A — gated by REQU-07 (No): Basecamp is delivered entirely as multi-tenant SaaS over HTTPS; no on-premises appliance, agent, or inbound firewall exception is required. |

### AI

The AI section is likewise gated off by the workbook (REQU-04 = No), and is nonetheless completed in full as a scoped disclosure: Basecamp ships no in-product AI, 37signals uses no AI on customer data, and the Anthropic/OpenAI entries on the subprocessor list are staff day-to-day tooling. Customers may connect their own AI agents to Basecamp (Bring-Your-Own-Agent) under their own credentials and their own AI provider's terms; that boundary is stated wherever a row would otherwise read as a missing control. In the filled workbook, rows whose dropdown offers no N/A keep an empty Answer cell and carry the position in Additional Information, per the workbook's instructions for gated rows.

| # | Question | Response | Additional information |
|---|---|---|---|
| AIQU-01 | Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months? | No | No machine learning operates in Basecamp on customer data, and none is planned within the next 12 months as of this answer. Disclosed for completeness: 37signals staff use commercial AI tools internally (no customer data involved), and customers may connect their own AI agents to their own account (Bring-Your-Own-Agent, BYOA) under their own credentials. |
| AIQU-02 | Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months? | No | Same basis as AIQU-01: no LLM operates in Basecamp on customer data, and none is planned within 12 months. The LLM vendors on the published Basecamp subprocessor list (Anthropic, OpenAI) are staff day-to-day tooling, not part of the solution. BYOA means the customer's own LLM agent, operating under the customer's own credentials and the customer's own AI provider's terms — not one 37signals operates. |
| AIGN-01 | Does your solution have an AI risk model when developing or implementing your solution's AI model?* | N/A | No in-product AI acts on customer data; there is no in-product AI to which an AI risk model would apply. No AI-specific risk model is claimed. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AIGN-02 | Can your solution's AI features be disabled by tenant and/or user?* | N/A | No in-product AI acts on customer data; there is no in-product AI feature to disable. BYOA is customer-initiated by design: nothing runs unless the customer connects an agent under their own credentials, and revoking those credentials ends it. |
| AIGN-03 | Have your staff completed responsible AI training?* | No | No responsible-AI training program exists; staff receive general security-awareness training only. Answered No rather than N/A: staff do use commercial AI tools internally (disclosed at AIQU-01), so the question applies even with no in-product AI — the gap is stated, not reclassified. |
| AIGN-04 | Please describe the capabilities of your solution's AI features. | None | Basecamp has no in-product AI features. Disclosure of the adjacent surface: Bring-Your-Own-Agent (BYOA) lets a customer connect their own AI agent (any agent that can run shell commands, or an MCP client) to their own Basecamp account through the Basecamp CLI/API; the agent acts under that customer's own credentials and account permissions, and under the customer's own AI provider's terms. 37signals hosts and runs no model. |
| AIGN-05 | Does your solution support business rules to protect sensitive data from being ingested by the AI model? | N/A | No in-product AI acts on customer data; there is no 37signals AI ingestion path to gate. For BYOA, a connected agent sees exactly what the connecting human's own account permissions allow, by design. |
| AIPL-01 | Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?* | N/A | No in-product AI acts on customer data. No AI governance policy is claimed; the governing statement is the Privacy Policy commitment that any use of AI with customer data would be disclosed there. |
| AIPL-02 | Have you identified and measured AI risks?* | N/A | No in-product AI acts on customer data; there is no in-product AI whose risks would be identified and measured. |
| AIPL-03 | In the event of an incident, can your solution's AI features be disabled in a timely manner?* | N/A | No in-product AI acts on customer data; no in-product AI feature exists to disable. General incident response applies to the API/CLI surface BYOA uses (account owners contacted within 24 hours; incident response owned by 37signals' operations and security teams), and a customer can revoke their own agent's credentials at any time. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AIPL-04 | If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?* | N/A | No in-product AI acts on customer data; no in-product AI feature exists to disable or re-enable. |
| AIPL-05 | Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)? | N/A | No in-product AI acts on customer data. No NIST AI RMF mapping is claimed. |
| AISC-01 | If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?* | N/A | No in-product AI acts on customer data; no model operated by or for 37signals holds customer data. Standard data-subject rights (including erasure) and retention timelines apply to 37signals' own systems. |
| AISC-02 | Is user input data used to influence your solution's AI model?* | N/A | No in-product AI acts on customer data; there is no 37signals model for user input to influence. Disclosed for completeness: 37signals does not train or fine-tune AI models on customer data. The staff-tooling vendors' commercial terms prohibit training on customer content — Anthropic's commercial terms state Anthropic may not train models on customer content from the services, and OpenAI's Services Agreement states OpenAI will not use customer content to develop or improve its services unless the customer explicitly agrees — and 37signals has opted into no training or data-sharing program. Standard vendor retention applies (no zero-data-retention agreement); both relationships are under click-through commercial terms, not negotiated agreements. |
| AISC-03 | Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?* | N/A | No in-product AI acts on customer data; no in-product AI feature exists to log. BYOA agents act under the connecting user's own credentials; general access logging and the bi-weekly staff data-access audits are unchanged. |
| AISC-04 | Please describe how you validate user inputs. | N/A | N/A for AI input: no in-product AI acts on customer data, so there is no AI input path to validate. The API/CLI surface BYOA uses is covered by the general application-security practices: OWASP-aligned code review, third-party penetration testing, and a public HackerOne bug bounty program. |
| AISC-05 | Do you plan for and mitigate supply-chain risk related to your AI features? | N/A | No in-product AI acts on customer data; no AI component is in the solution's supply chain. The staff-tooling AI vendors are governed like any subprocessor: written data-processing terms, listing on the published subprocessor list, and the DPA's 10-business-day objection window. |

| # | Question | Response | Additional information |
|---|---|---|---|
| AIML-01 | Do you separate ML training data from your ML solution data?* | N/A | 37signals trains no machine-learning models and holds no ML training corpus, so there is no training data to separate; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-02 | Do you authenticate and verify your ML model's feedback?* | N/A | 37signals trains and operates no ML model, so there is no model feedback loop to authenticate or verify; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-03 | Is your ML training data vetted, validated, and verified before training the solution's AI model? | N/A | 37signals trains no machine-learning models and holds no ML training corpus, so there is no training data to vet, validate, or verify; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-04 | Is your ML training data monitored and audited? | N/A | 37signals trains no machine-learning models and holds no ML training corpus, so there is no training data to monitor or audit; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-05 | Have you limited access to your ML training data to only staff with an explicit business need? | N/A | 37signals trains no machine-learning models and holds no ML training corpus, so there is no training data to restrict access to; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-06 | Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features? | N/A | 37signals trains and operates no ML model and ships no ML-related features, so there is no model to defend; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-07 | Do you make your ML model transparent through documentation and log inputs and outputs? | N/A | 37signals trains and operates no ML model, so there is no model to document or whose inputs and outputs would be logged; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |
| AIML-08 | Do you watermark your ML training data? | N/A | 37signals trains no machine-learning models and holds no ML training corpus, so there is no training data to watermark; no in-product AI acts on customer data. The staff-tooling vendors' foundation models are consumed as delivered, under terms that prohibit training on customer content (see AISC-02). |

| # | Question | Response | Additional information |
|---|---|---|---|
| AILM-01 | Do you limit your solution's LLM privileges by default? * | N/A | The solution operates no LLM; no in-product AI acts on customer data. Disclosed for the BYOA surface: a connected agent inherits the connecting human's own account permissions — an agent can do anything in Basecamp the connecting user can do — under the customer's own credentials; scoping what an agent may do is the customer's choice of account, permissions, and agent configuration. |
| AILM-02 | Is your LLM training data vetted, validated, and verified before training the solution's AI model?* | N/A | 37signals trains or fine-tunes no LLM, so there is no LLM training data to vet, validate, or verify; no in-product AI acts on customer data (see AISC-02 and the AIML rows). |
| AILM-03 | Do any actions taken by your solution's LLM features or plugins require human intervention?* | N/A | The solution has no LLM features or plugins; no in-product AI acts on customer data. For BYOA, per-action approval is a property of the customer's own agent runtime; the customer's decisions are which agent to connect, under which account, and when to revoke it. |
| AILM-04 | Do you limit multiple LLM model plugins being called as part of a single input?* | N/A | The solution has no LLM plugins; no in-product AI acts on customer data. BYOA orchestration happens entirely in the customer's own agent runtime — Basecamp works with any AI agent that can run shell commands. |
| AILM-05 | Do you limit your solution's LLM resource use per request, per step, and per action? | N/A | The solution operates no LLM; no in-product AI acts on customer data, so there is no LLM resource use to limit. |
| AILM-06 | Do you leverage LLM model tuning or other model validation mechanisms? | N/A | 37signals tunes no model and operates no LLM; no in-product AI acts on customer data (see AILM-02). |

## Privacy

| # | Question | Response | Additional information |
|---|---|---|---|
| PRGN-01 | Does your solution process FERPA-related data? | Yes | Basecamp customers and their end users control what content is uploaded, which may include FERPA-covered education records; 37signals acts as a processor under its DPA for such data. The DPA's FERPA provision (§12, FERPA (US Schools), mirrored at 37signals.com/policies/privacy/regulations/ferpa) maps the DPA's terms to the school-official standard — documented-instructions-only processing, institutional control, no onward disclosure, return and deletion — and commits: if a school designates 37signals as a school official with a legitimate educational interest, 37signals accepts that designation and agrees to use and maintain education records under the conditions of 34 CFR §99.33(a). The designation itself remains the institution's FERPA office's determination under 34 CFR §99.31(a)(1)(i)(B). |

| # | Question | Response | Additional information |
|---|---|---|---|
| PRGN-02 | Does your solution process GDPR-related or PIPL-related data? | Yes for GDPR; No for PIPL | 37signals processes GDPR-regulated personal data whenever EEA/UK/Swiss individuals use the service, which is why 37signals maintains a GDPR DPA with Standard Contractual Clauses. 37signals does not process data in or from China and does not represent PIPL compliance. |
| PRGN-03 | Does your solution process personal data regulated by state law(s) (e.g., CCPA)? | Yes | Basecamp customers may store California residents' personal information as content. 37signals maintains a CCPA Notice covering U.S. state privacy law and does not sell or share personal information as defined by the CCPA. |
| PRGN-04 | Does your solution process user-provided data that may contain regulated information? | Yes | By design: Basecamp stores whatever content customers and their end users choose to upload, which may include regulated personal data. 37signals does not inspect, classify, or limit that content (Privacy Policy, "Product interactions"). |
| PRGN-05 | Web Link to Product/ Service Privacy Notice | https:// 37signals.com/ policies/privacy | Canonical URL for the 37signals Privacy Policy. |
| PCOM-01 | Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?* | No | The Security Overview states: "To date, we've never had a data breach. We have processes and defenses in place to keep our streak of 0 data breaches going." This is a self-attested but explicit public claim; no independent breach-notification record was found. |
| PCOM-02 | Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.* | See additional information | 37signals runs Basecamp under a single published privacy program applied to every customer: a GDPR-grade DPA with Standard Contractual Clauses (Module 2/3, Irish governing law/DPC); a published, product-specific subprocessor list with a 10-business-day objection window; engineering-enforced staff access controls (console1984/audits1984 — consented, logged, bi-weekly-audited console access, the sole documented exception being abuse/policy-violation investigation, a measure of last resort that does not always require prior customer consent — see PDAT-07), plus at-work encryption for Basecamp 5 so engineers cannot casually view customer content; a public commitment to never sell personal data; and a public breach-notification commitment. The program does not include a dedicated privacy office, a formally designated DPO, or PIPL/China-specific controls (see PCOM-04, INTL-02, INTL-05). |

| # | Question | Response | Additional information |
|---|---|---|---|
| PCOM-03 | Have you had any violations of your internal privacy policies or violations of applicable privacy law in the past 36 months? | No | No enforcement actions, consent decrees, or violations were located in public search; this is an absence-of-evidence answer. |
| PCOM-04 | Do you have a dedicated data privacy staff or office? | No | 37signals does not maintain a dedicated data privacy staff or office, consistent with the absence of any published DPO or privacy-office designation (see INTL-02). |
| PDOC-01 | If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle? | N/A | The question is conditional on having completed a SOC 2 audit; 37signals has not. The Security Overview states: “37signals LLC itself has not completed a SOC audit.” |
| PDOC-02 | Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)? | Yes | GDPR: 37signals maintains a full GDPR DPA with Standard Contractual Clauses, and the Privacy Policy states that 37signals strives to apply the same data rights to all customers, regardless of their location. |
| PDOC-03 | Does your employee onboarding and offboarding policy include training of employees on information security and data privacy? | Yes | Onboarding includes information-security training and confidentiality agreements: all employees and contractors sign confidentiality agreements before receiving access to code or customer data, and are trained on security best practices. There is no separate formal data-privacy training program (see PRPO-06/07); data-privacy expectations are enforced through engineering controls instead — production access to customer data requires explicit per-session consent and is logged and audited on a bi-weekly cycle. |
| PTHP-01 | Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?* | Yes | 37signals enters a written agreement with every subprocessor containing data-protection obligations no less protective than the 37signals DPA (DPA §5.1). |

| # | Question | Response | Additional information |
|---|---|---|---|
| PTHP-02 | Do you perform privacy impact assessments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects? | No | There is no published process for assessing subprocessors' own privacy programs beyond contractual flow-down of data-protection obligations. |
| PCHG-01 | Does your change management process include privacy review and approval? | Yes | Per internal SDLC/change-management policy. This is not independently audited (37signals has not completed a SOC 2 audit — see PDOC-01); the policy document is internal and can be made available directly or under NDA upon request. |
| PCHG-02 | Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved? | Yes | Per internal policy; not independently audited. The policy document is internal, available directly or under NDA on request. |
| PDAT-01 | Do you collect, process, or store demographic information?* | No | As to what 37signals itself collects, processes, or uses: account identity data — name, email address, and optionally a company name and profile picture (the Privacy Policy's illustrative "such as" language) — none of it demographic. Customers can place demographic data in their own content; Basecamp stores and processes such content as a processor on the customer's behalf (see PRGN-01 through PRGN-04) and does not inspect, classify, or use it. |
| PDAT-02 | Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?* | No | No biometric or genetic data category is listed in the Privacy Policy; the optional profile photo is not biometric processing. |
| PDAT-03 | Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?* | No | Under the DPA (§2.3.3.ii), 37signals will not attempt to re-identify or link de-identified data without customer authorization. |

| # | Question | Response | Additional information |
|---|---|---|---|
| PDAT-04 | Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving? | Yes | Basecamp's data infrastructure is US-based: primary data centers in Chicago, IL and Ashburn, VA, with a read-only outpost in San Jose, CA. Data from customers outside the US (including the EEA/UK) is transferred to and stored in the United States under the 37signals DPA and Standard Contractual Clauses. Basecamp has no EU/EEA data center — the Amsterdam outpost belongs to HEY, a different 37signals product. |
| PDAT-05 | Do you capture device information (e.g., IP address, MAC address)? | Yes | The Privacy Policy states that 37signals logs the full IP address used to sign up a product account, and separately logs all account access by full IP address for security and fraud prevention purposes (i.e., every login). |
| PDAT-06 | Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)? | Yes | 37signals may load an ad-company script that sets a third-party cookie, and separately uses persistent first-party cookies and some third-party cookies to store preferences, perform A/B testing, and support analytics (Privacy Policy, Advertising and Cookies section). |
| PDAT-07 | Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means? | Yes | In limited, logged, and audited circumstances. 37signals' default is no employee access to customer content. Access requires explicit per-session consent, is recorded via console1984, and is audited bi-weekly via audits1984; Basecamp 5 additionally encrypts data at-work so engineers cannot casually view content during normal operation. The narrow exception is abuse/policy-violation investigation, a measure of last resort that does not always require prior customer permission. |
| PDAT-08 | Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies? | Yes as to laws and regulations; No as to customer-institution-specific internal policies | 37signals processes personal data under GDPR (via its DPA incorporating Standard Contractual Clauses, Module 2/3, Irish governing law), the CCPA, and other U.S. state privacy laws, consistent with its Privacy Policy. It does not adapt its practices to each institution's individual internal privacy policy; institution-specific requirements would need to be negotiated contractually (see PRPO-04). |
| PRPO-01 | Do you have a documented privacy management process? | Yes | Assembled from several published, engineering-enforced artifacts — the DPA's subprocessor process, the console1984/audits1984 consent-and-audit workflow, and the Privacy Policy — rather than one single named "privacy management program" document. |
| PRPO-02 | Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)? | Yes | Default-no-access design, a per-session consent requirement for production data access, console encryption-by-default, and at-work encryption for Basecamp 5. 37signals does not use the phrase "privacy by design" in any published material; the answer is supported by substance, not by a matching label. |

| # | Question | Response | Additional information |
|---|---|---|---|
| PRPO-03 | Will you comply with applicable breach notification laws? | Yes | 37signals commits contractually (DPA §7) to notify customers without undue delay, and in compliance with applicable data protection law, after becoming aware of a Personal Data Incident. Separately, the Security Overview — which the DPA's definition of "Security, Privacy and Architecture Documentation" expressly incorporates by reference — commits to contacting the account owner within 24 hours of an incident. These are complementary, not conflicting: the 24-hour figure is the general incident-notification commitment (security and availability incidents); the DPA clause is the GDPR-specific Personal Data Incident notification standard. |
| PRPO-04 | Will you comply with the institution's policies regarding user privacy and data protection? | No | A standard limitation for a multi-tenant SaaS vendor, consistent with PDAT-08: 37signals applies one published privacy program to all customers rather than adopting each institution's internal policies. |
| PRPO-05 | Is your company subject to the laws and regulations of the institution's geographic region? | Yes | As to United States federal and Illinois state law (DPA Annex I), plus the EU/UK/Swiss and U.S. state privacy laws the DPA contractually applies. 37signals is not separately subject to each institution's own state or regional laws — see PPPR-03. |
| PRPO-06 | Do you have a privacy awareness/ training program?* | No | There is no separate, formal privacy-awareness training program distinct from general security training. All workers sign confidentiality agreements and receive security-best-practices training (see PDOC-03); production access to personal data additionally requires explicit per-session consent and is logged and audited by engineering controls rather than governed by a training curriculum. |
| PRPO-07 | Is privacy awareness training mandatory for all employees? | No | Consistent with PRPO-06; confidentiality agreements — not privacy training specifically — are mandatory. |
| PRPO-08 | Is AI privacy and ethics awareness/ training required for all employees who work with AI? | No | No AI-specific privacy/ethics training program is documented; staff who use AI tools (Claude, ChatGPT) in day-to-day work are covered by the general security-awareness training only. The N/A option (for providers whose staff do not use AI) is not taken: staff do use AI tools internally, even though no AI operates on customer data. |
| PRPO-09 | Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)? | No | The Privacy Policy publishes a "Right to not Be Subject to Automated Decision-Making," consistent with no such automated decisioning occurring in the product. |

| # | Question | Response | Additional information |
|---|---|---|---|
| PRPO-10 | Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests? | No | Consistent with PRPO-09; with no fully automated decision-making in the product, no such management process is needed. |
| PRPO-11 | Do you have a documented policy for sharing information with law enforcement? | Yes | The Privacy Policy states: “Our policy is to not respond to government requests for user data unless we are compelled by legal process or in limited circumstances in the event of an emergency request,” and that data is provided only if U.S. law enforcement authorities have the necessary warrant, criminal subpoena, or court order. |
| PRPO-12 | Do you share any institutional data with law enforcement without a valid warrant or subpoena? * | No | Policy is to not respond to government requests for user data unless compelled by a valid warrant, criminal subpoena, or court order. The one exception stated in the Privacy Policy’s law-enforcement clause — limited emergency circumstances as described there — is disclosed alongside the No: it is the policy’s own narrowly-scoped emergency provision, not a practice of warrantless sharing. |
| PRPO-13 | Does your incident response team include a privacy analyst/officer? | No | Consistent with PCOM-04: 37signals has no dedicated privacy staff or office, so the incident response team does not include a designated privacy analyst/officer. |
| INTL-01 | Will data be collected from or processed in or stored in the European Economic Area (EEA)? | Yes | Data is collected from EEA data subjects. It is not stored or processed within the EEA — Basecamp’s infrastructure is entirely US-based (Chicago, IL; Ashburn, VA; and a read-only outpost in San Jose, CA). EEA-originated data is transferred to and processed in the US under the DPA and GDPR Standard Contractual Clauses. |
| INTL-02 | Do you have a data protection officer (DPO)? | No | 37signals has not published a formally designated Data Protection Officer. Privacy inquiries and DPA questions are directed to privacy@37signals.com (DPA §4.4 — a contact channel, not a DPO title). Consistent with PCOM-04 (no dedicated privacy staff/office). |
| INTL-03 | Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution? | Yes | By signing the 37signals Agreement, the customer and 37signals are deemed to have executed the EU Standard Contractual Clauses (Module 2 controller-to-processor and Module 3 processor-to-processor, as applicable), with Irish law and the Irish Data Protection Commission as governing law and forum (DPA §11.2). |
| INTL-04 | Will data be collected from or processed in or stored in China? | No | No infrastructure, storage, processing, or subprocessor is located in China; all nine published Basecamp subprocessors are US-based. Users may access Basecamp from anywhere, including China — content submitted by users located outside the United States is transferred to and stored in the United States per the Privacy Policy; 37signals imposes no geographic access restriction. |

| # | Question | Response | Additional information |
|---|---|---|---|
| INTL-05 | Do you comply with PIPL security, privacy, and data localization requirements? | No | Consistent with INTL-04: 37signals does not process data in or from China, and no PIPL-related statement appears in any published material. |
| DRPV-01 | Have you performed a Data Privacy Impact Assessment for the solution/project? | No | No formal DPIA has been performed. In our assessment, 37signals' processing (SaaS project-management/ collaboration content, determined entirely by the customer) does not appear to meet GDPR Art. 35 high-risk triggers (no systematic large-scale profiling, no large-scale special-category processing, no public-area monitoring) as a general matter — this is our own analysis, not a position 37signals has published. 37signals commits under its DPA (§2.3.5) to provide reasonable assistance if a customer needs to perform its own DPIA. |
| DRPV-02 | Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is collected, used, retained, and disclosed? | Yes | The Privacy Policy is structured around exactly this: what is collected and why, and how it is used, retained, and disclosed. |
| DRPV-03 | Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information? | Yes | Mobile permissions are requested only with optional user consent, and cookie controls are described in the Privacy Policy. |
| DRPV-04 | Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in the privacy notice? | Yes | The Privacy Policy's guiding principle is to collect only what is needed. |
| DRPV-05 | Do you have a documented list of personal data your service maintains? | Yes | Described narratively in the Privacy Policy's "What we collect and why" section (identity/access, billing, product content, geolocation, analytics, cookies, correspondence, mobile permissions) rather than as a standalone itemized table. |

| # | Question | Response | Additional information |
|---|---|---|---|
| DRPV-06 | Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter appropriately dispose of such information? | Yes | If an account is deleted, content is deleted within 60 days; deleted content is kept in an accessible trash for about 25 days and purged from all systems and logs within 90 days (Privacy Policy). This is consistent with the Security Overview's 30-day active/60-day backup figures once read as outer-bound vs. phased timelines. |
| DRPV-07 | Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)? | Yes | The Privacy Policy publishes a Right of Access and a Right to Correction; many rights can be exercised directly by signing in and updating account information. |
| DRPV-08 | Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the individual? | Yes | With a caveat: 37signals never sells data and follows a subprocessor-only sharing model. One narrow exception exists (the ad-exclusion hash disclosure, see DRPV-13), and it is disclosed in the Privacy Policy itself. |
| DRPV-09 | Do you protect personal information against unauthorized access (both physical and logical)? | Yes | VPN plus 2FA for system access, encryption in transit and at rest, at-work encryption for Basecamp 5, biometric-locked and 24/7-staffed data centers, and console1984/audits1984 access logging and auditing (Security Overview). |
| DRPV-10 | Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice? | Yes | Scoped: self-service mechanisms exist for individuals to review and correct their own information; accuracy of customer-controlled content is otherwise the customer's/ data subject's responsibility per the DPA (§2.2.2). |
| DRPV-11 | Do you have procedures to address privacy-related noncompliance complaints and disputes? | Yes | Data subjects have a published "Right to Complain," and privacy inquiries route to privacy@37signals.com (DPA §4.4). A detailed internal complaint-handling procedure is not separately published. |
| DRPV-12 | Do you "anonymize," "de-identify," or otherwise mask personal data? | Yes | The Privacy Policy states: "We may aggregate and/or de-identify information collected through the services." |

| # | Question | Response | Additional information |
|---|---|---|---|
| DRPV-13 | Do you or your subprocessors use or disclose “anonymized,” “de-identified,” or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)? | Yes | In one narrow, published respect: 37signals may disclose a one-way hash of a Basecamp account holder’s email address to ad companies solely to exclude that person from seeing 37signals’ own ads (suppression, not targeting or profiling). This applies to an institution’s own Basecamp users’ account emails, not merely to visitors of 37signals’ marketing site; it does not touch Basecamp project content and is not a sale under the CCPA. Separately, 37signals states it may use de-identified or aggregated data “for any purpose, including marketing or analytics” (Privacy Policy). |
| DRPV-14 | Do you certify stop-processing requests, including any data that is processed by a third party on your behalf? | Yes | Upon request: on termination, 37signals returns and (where legally permitted) deletes Personal Data per its published retention timelines; certification of deletion under the GDPR SCCs is provided only upon the customer’s request, not automatically (DPA §8, §11.8). |
| DRPV-15 | Do you have a process to review code for ethical considerations? | No | No public evidence of a formal ethics-in-code-review process. |
| DPAI-01 | Does your service use AI for the processing of institutional data? | N/A | No in-product AI acts on customer data: Basecamp has no in-product AI, and 37signals does not use AI with customer data. The Anthropic/OpenAI entries on the Basecamp subprocessor list are staff day-to-day tooling that does not process customer content. Any AI processing of a customer’s own data through bring-your-own-agent (BYOA) is performed by the customer’s own agent, under the customer’s own credentials and AI provider terms, outside 37signals’ processing. |
| DPAI-02 | Is any institutional data retained in AI processing?* | N/A | No institutional data enters any AI processing operated by 37signals (see DPAI-01), so none is retained in AI processing. |
| DPAI-03 | Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?* | N/A | No in-product AI acts on customer data (see DPAI-01). For completeness: every subprocessor, the staff-tooling AI vendors included, is bound by a written agreement with data-protection obligations not less protective than the DPA (§5.1), and the AI vendors’ commercial terms prohibit training on customer content. |
| DPAI-04 | Will institutional data be processed through a third party or subprocessor that also uses AI? | N/A | No subprocessor processes institutional data on 37signals’ behalf using AI; no in-product AI acts on customer data (see DPAI-01). |

| # | Question | Response | Additional information |
|---|---|---|---|
| DPAI-05 | Is AI processing limited to fully licensed commercial enterprise AI services? | N/A | No AI processing of institutional data occurs (see DPAI-01). Staff tooling uses the vendors' commercial services under click-through commercial terms (not negotiated agreements); no customer data is involved. |
| DPAI-06 | Will institutional data be used or processed by any shared AI services? | N/A | No institutional data is used or processed by any shared AI services; no in-product AI acts on customer data (see DPAI-01). |
| DPAI-07 | Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing? | N/A | No 37signals AI ingestion path exists to safeguard, since no in-product AI acts on customer data (see DPAI-01). The operating rule is that staff AI tooling is not used on customer data; separately, staff access to customer data is need-to-know, per-session consent-gated, and bi-weekly audited, which limits and detects access but is not claimed as a technical block on what an authorized person could paste into a tool — no DLP-style AI-ingestion control exists. |
| DPAI-08 | Do you provide choice to the user to opt out of AI use? | N/A | There is no in-product AI use to opt out of (see DPAI-01). BYOA is entirely customer-initiated: nothing runs unless the customer connects an agent, and revoking the agent's credentials ends it. |