BeamIdea Security Overview

Last updated: 2026-01-18

This document provides a concise overview of security and privacy measures for BeamIdea. It is informational only and does not modify the terms of any signed agreement. In the event of a conflict, the applicable agreement (including the Security Addendum, DPA and SLA) prevails.

1. Security at a glance

- Security program aligned with widely used controls frameworks (including SOC 2 Type II style controls), including periodic risk assessment.
- Access control based on least privilege and role-based permissions (RBAC); administrative access protected by MFA/SSO where applicable.
- Encryption in transit (TLS 1.2 or higher) and encryption at rest (AES-256 or equivalent).
- Logical segregation of Customer Data by tenant.
- Centralized logging and monitoring; security-relevant audit logs are retained for at least 12 months.
- Encrypted backups performed daily; business continuity targets defined in customer-facing documentation.
- Documented incident response process, including customer notification for confirmed personal data incidents within contractual timelines.

2. Governance and personnel security

BeamIdea is operated under an internal security program that includes policies, role definitions, training and access governance. Access to production systems is restricted to authorized personnel and is granted on a least-privilege basis.

- Security training for personnel with access to systems or Customer Data.
- Background checks where legally permitted and appropriate for the role.
- Formal offboarding to remove access promptly when personnel change roles or leave.

3. Access control and authentication

BeamIdea uses role-based access control (RBAC) to ensure users and administrators can access only what they need. Administrative access is protected with strong authentication controls.

- RBAC and least-privilege permissions for application and infrastructure access.
- Support for enterprise identity (SSO) where applicable (e.g., SAML/OIDC), subject to customer configuration.

- Multi-factor authentication (MFA) for administrative access and internal privileged accounts where applicable.
- Session and access controls designed to reduce the risk of unauthorized access.

4. Data protection and privacy

BeamIdea processes Customer Data to provide the service, support customers and maintain platform security. Data categories may include company and user account information, user-generated content (idea proposals and discussions), and usage/security logs.

- Encryption in transit: TLS 1.2 or higher.
- Encryption at rest: AES-256 or equivalent provider-managed encryption.
- Logical segregation: Customer Data is separated by tenant.
- Data minimization: processing is limited to what is necessary to provide the service.
- Retention and deletion: Customer Data is deleted or returned following termination in accordance with contractual terms, typically within 90 days unless legal retention applies.

5. Application and infrastructure security

Security controls are applied across the development lifecycle and the hosting environment to reduce the likelihood of vulnerabilities and to support timely remediation.

- Secure development practices such as peer review and change control for production changes.
- Vulnerability management including scanning and patching processes.
- Third-party security testing (such as penetration testing) performed periodically, with remediation tracked by severity.
- Secrets management practices to avoid hardcoded credentials and reduce exposure.
- Protective controls such as rate limiting and other safeguards as appropriate for the service.

6. Logging, monitoring and audit trails

BeamIdea maintains centralized logging and monitoring to detect operational issues and security-relevant events. Audit logs support investigations and customer support where appropriate.

- Centralized monitoring and alerting for service health and anomalous activity.
- Security-relevant audit logs retained for at least 12 months.
- Time synchronization and access controls applied to logging systems.

7. Business continuity and disaster recovery

BeamIdea maintains backup and recovery practices designed to support service continuity. Backup, recovery, and continuity targets are described in customer-facing documentation and may vary by deployment.

- Encrypted backups performed daily.
- Periodic restore tests to validate backup integrity and recovery procedures.
- Continuity objectives (e.g., RPO/RTO) documented for the service and reviewed periodically.

8. Incident response and security notifications

BeamIdea maintains an incident response process for identifying, triaging and remediating security incidents. For confirmed personal data incidents, customers are notified without undue delay and within contractual timelines.

- Documented incident classification and escalation paths.
- Actions to contain, eradicate and recover from incidents.
- Customer notification for confirmed personal data incidents within contractually agreed timelines (commonly within 72 hours of confirmation).

9. Subprocessors

BeamIdea may use subprocessors to provide specific components of the service (e.g., hosting, analytics or AI processing). Subprocessors are engaged under written agreements with appropriate security and confidentiality obligations.

- Security review and due diligence prior to onboarding subprocessors.
- Contractual requirements for confidentiality and security measures.
- Subprocessor list and change process are provided in the applicable DPA/appendices.

10. Customer responsibilities (shared responsibility)

Security is shared. Customers are responsible for managing their users and device environment, including identity provider settings, endpoint/device management (e.g., MDM), and internal policies. BeamIdea is responsible for the security of the hosted service and its underlying infrastructure within the scope of the service.

- Configure SSO and MFA policies (where supported) and manage user lifecycle (joiners/movers/leavers).
- Use Apple Business Manager and an MDM to enable rapid and controlled device deployment where required.

- Follow the Acceptable Use Policy and ensure users do not upload prohibited content or data categories.

11. Acceptable use and abuse prevention

To protect customers and the service, BeamIdea prohibits abusive or unlawful use, including attempts to bypass security controls or disrupt service availability.

- No malware, unauthorized scanning, denial-of-service attempts, or attempts to circumvent access controls.
- No large-scale scraping or harvesting of data beyond authorized use.
- Restrictions on certain sensitive or regulated data unless explicitly agreed in writing.

12. Service reliability (SLA summary)

BeamIdea provides service availability commitments and support response targets as described in the SLA. Scheduled maintenance windows and service credits may apply as outlined in the SLA.

- Target monthly availability: 99.5% (subject to SLA definitions and exclusions).
- Scheduled maintenance: typically during off-hours; advance notice applies per SLA.
- Support hours and incident response targets defined by severity level.

13. Assurance and customer requests

Customers may request additional information as part of their vendor security review. Where applicable and available, we can provide standard security documentation (e.g., pen test summaries or attestations) under appropriate confidentiality terms. Audit and information rights are governed by the signed agreements.

14. Security contact

Security and privacy inquiries:

- Erik Arlen Fitch (CTO) - erik@fitchhardt.com
- General contact - contact@fitchhardt.com