BOULAY

Zoobean, Inc. d/b/a Beanstack

SOC 3 Report

for the

Beanstack Digital Platform

An Independent Service Auditor's Report on Controls Relevant to Security

January 1, 2026 to June 30, 2026

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Zoobean, Inc. d/b/a Beanstack:

Scope

We have examined Zoobean, Inc. d/b/a Beanstack's ("Beanstack" or the "service organization") accompanying assertion titled "Management's Assertion" (assertion) that the controls within the Beanstack Digital Platform were effective throughout the period of January 1, 2026 to June 30, 2026, to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Beanstack uses Heroku and Amazon Web Services (the "subservice organizations") to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Beanstack, to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Beanstack's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Beanstack, to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Beanstack's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Beanstack is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved. Beanstack has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Beanstack is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Beanstack Digital Platform were effective throughout the period of January 1, 2026 to June 30, 2026, to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Minneapolis, Minnesota
August 19, 2026

SECTION II

MANAGEMENT'S ASSERTION

Docusign Envelope ID: 091DC91D-78E6-8D67-8334-5A365D8D3B57

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Zoobean, Inc. d/b/a Beanstack's ("Beanstack") Beanstack digital platform throughout the period of January 1, 2026 to June 30, 2026, to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in Section III entitled "Description of the Boundaries of the Beanstack Digital Platform" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system through the period of January 1, 2026 to June 30, 2026, to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved based on the applicable trust services criteria. Beanstack's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV entitled "Description of the Principal Service Commitments and System Requirements of the Beanstack Digital Platform".

Beanstack uses Heroku and Amazon Web Services (the "subservice organizations") to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Beanstack, to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Beanstack's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Beanstack, to achieve Beanstack's service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Beanstack's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period of January 1, 2026 to June 30, 2026, to provide reasonable assurance that Beanstack's service commitments and system requirements were achieved based on the applicable trust services criteria.

Felix Brandon Lloyd

Felix Brandon Lloyd
Chief Executive Officer
Zoobean, Inc. d/b/a Beanstack

SECTION III

DESCRIPTION OF THE BOUNDARIES OF THE BEANSTACK DIGITAL PLATFORM

DESCRIPTION OF THE BOUNDARIES OF THE BEANSTACK DIGITAL PLATFORM

Company Background

Zoobean, Inc. d/b/a Beanstack ("Beanstack" or "the Company") is a software as a service (SaaS) company that helps educators, librarians, and organizations encourage reading by providing tools to build, manage, and promote reading challenges for their communities. The platform motivates users to reach reading goals by tracking when, how much, and what they read across web and mobile applications.

Beanstack primarily serves K-12 public school districts, public library systems, and educational institutions. The platform enables administrators to track community-wide reading engagement, manage customized reading programs, and generate reader analytics, operating as a cloud-hosted solution designed to support secure student and reader participation.

Description of Services Provided

School and District Functionality

The Beanstack Digital Platform for schools uses proven gamification principles and modern reading accountability tools that motivate students to read and grow school districts' reading cultures.

District administrators can:

- Manage reading challenges
  - Create reading challenges for all students or specific grade bands
  - Use Beanstack's extensive template library or create a custom challenge
  - Automate monthly challenge publishing
- Customize reading integrity settings
  - Set logging limits and warning levels
  - Activate and customize friends and leaderboards
  - Set logging requirements (e.g., including a book title)
  - Validate and freeze student readers
- Gain insights from Book Talks with Benny
  - View AI-generated summary and analysis of student book talks
  - View AI-generated integrity and engagement flags
  - See full student conversations with Benny
- Create and manage rewards, tickets, and drawings
- Set school-wide community reading goals
- View, review, and approve classroom library titles across the school
- Establish tandem connections with a public library or libraries
- View and manage classroom library collections

School administrators can:

- Manage reading challenges
  - Create reading challenges for all students or specific grade bands
  - Use Beanstack's extensive template library or create a custom challenge
  - Automate monthly challenge publishing
- Customize reading integrity settings
  - Set logging limits and warning levels
  - Activate and customize friends and leaderboards
  - Set logging requirements (e.g., including a book title)
  - Validate and freeze student readers

- Gain insights from Book Talks with Benny
    - View AI-generated summary and analysis of student book talks
    - View AI-generated integrity and engagement flags
    - See full student conversations with Benny
- Create and manage rewards, tickets, and drawings
- Set school-wide community reading goals
- View, review, and approve classroom library titles across the school
- Establish tandem connections with a public library or libraries
- View and manage classroom library collections

Teachers can:

- Access reporting and insights for their rostered students
    - View and customize insights (by classroom)
    - View and customize leaderboards (by classroom and readers)
    - Visualize student daily reading habits for each classroom with the Daily Reading Tracker
    - View and take action on student log sessions flagged for review, including verifying and freezing students
    - Access Lexile Insights for each classroom
    - Customize and download reports; schedule automated report delivery via email
- Log reading for any rostered classroom or student
- Participate as a reader
    - Log own reading, earn badges and streaks
    - Add students and staff as friends
    - Compete with students and staff on leaderboards
- Moderate book reviews for rostered students
- Create classroom library collections

Students can:

- Log reading minutes, books, and/or pages
- Engage in Book Talks with Benny after completing a book or logging an amount of reading over a site's warning level
- Participate in reading challenges
- Earn badges and achievements
- Earn streaks
- Add and accept student and staff friend invitations
- Compete on friends, grades, and school leaderboards
- View reading log history
- View their teachers' classroom library collections

All reader functionality is available on the Beanstack web and mobile applications.

Rostering & SSO Integrations for School Buildings and Districts

Rostering integrations are available to all school partners and automate account creation and provide single sign-on for students, teachers, and staff. Schools that do not use one of these rostering services can roster students via the manual CSV import functionality.

Service	Capabilities
Clever	Rostering and SSO
ClassLink	Rostering and SSO
Skyward	Rostering
RapidIdentity	Rostering and SSO
Aeries	Rostering

Service	Capabilities
Google	SSO
Microsoft	SSO
Wonde	Rostering

Public Library Functionality

The Beanstack digital platform for libraries empowers librarians to run digital reading programs, including for summer reading, 1,000 Books Before Kindergarten, and a wide range of programs.

Library administrators can:

- Manage reading challenges
    - Create reading challenges for all community members or specific groups (including staff and age/grade bands)
    - Use Beanstack's extensive template library or create a custom challenge
- Customize registration and other site settings
- Create and manage rewards, tickets, and drawings
- Establish tandem connections with a public library or libraries
- Set system-wide community reading goal
- Access system-wide reporting and insights
    - View and customize insights (by grade/age, branch, school)
    - Customize and download reports from extensive library of options; schedule automated report delivery via email
- Moderate book reviews
- Manage participants
    - Create and edit accounts and readers
    - Log reading and other actions for participants
    - Redeem incentives for readers
- Participate as a reader
    - Log own reading, earn badges and streaks
    - Add students and staff as friends
    - Compete with students and staff on leaderboards

Community members can:

- Log reading minutes, books, pages, and/or days
- Participate in reading challenges
- Earn badges and achievements
- Earn streaks
- Add and accept friend invitations and compete with friends on leaderboards
- View reading log history

All reader functionality is available on the Beanstack web and mobile applications.

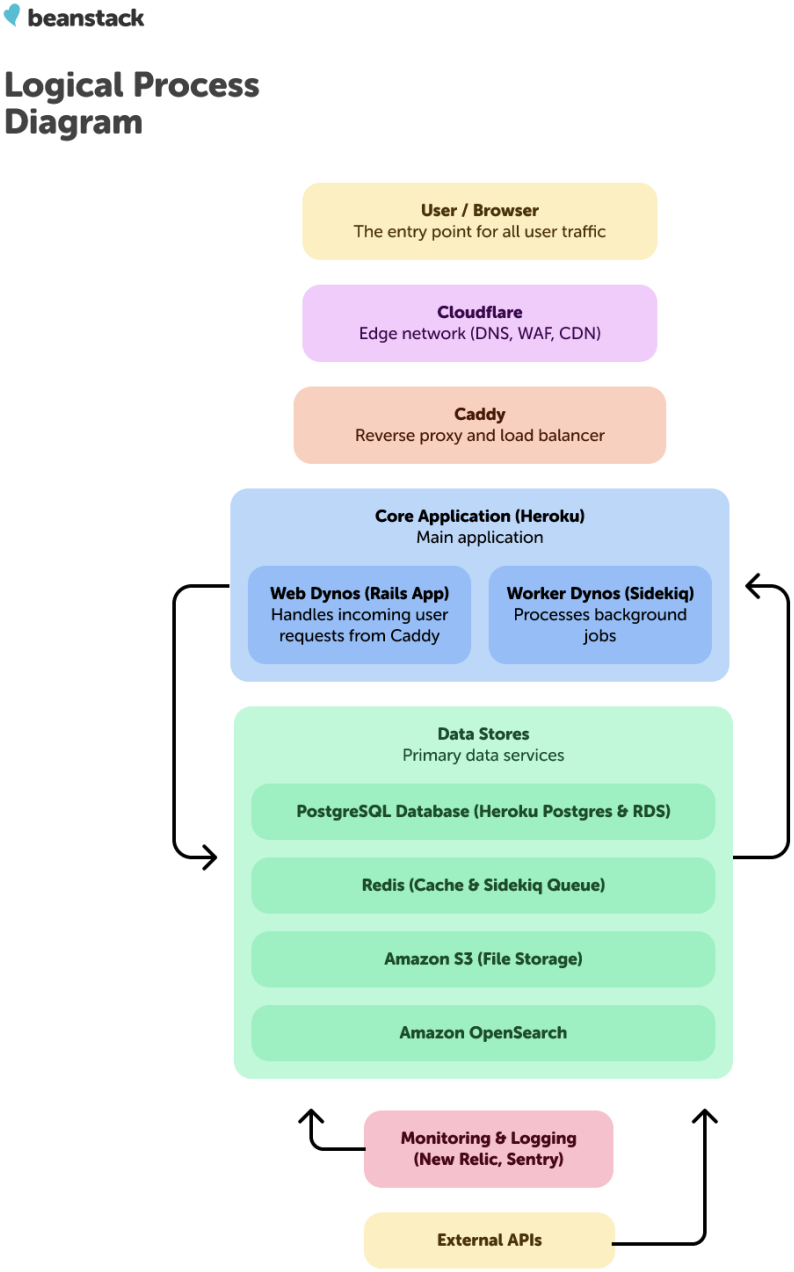
System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, data, and procedures.

Components of the System

Infrastructure

Beanstack uses Heroku and Amazon Web Services (AWS) to provide cloud computing and data center hosting services. The key infrastructure components are noted in the system diagram and table below.



Component	Purpose
Heroku Platform (PaaS)	The primary Platform-as-a-Service used for hosting the application web and worker dynos. It manages the runtime environment and scaling.
Cloudflare	Serves as the edge network, providing Domain Name Service (DNS), Web Application Firewall (WAF), and Content Delivery Network (CDN) services to protect and accelerate traffic.
Caddy Reverse Proxy	A self-managed reverse proxy used for load balancing and an extra layer of WAF.

Component	Purpose
Simple Storage Service (S3)	Offers secure, scalable object storage for data archiving, backup, and application support with high durability and availability.
Elastic Compute Cloud (EC2)	Delivers scalable virtual servers for compute-intensive workloads, enabling flexible deployment of applications and services.
Elastic Container Service (ECS)	Orchestrates containerized applications using a fully managed service, supporting scalability and automation.
Elastic Load Balancing	Distributes incoming network traffic across multiple targets to ensure high availability and fault tolerance.
Relational Database Service (RDS)	Provides managed relational database instances with automated backups, patching, and scaling to support application data needs.
Redis	Provides high-speed, scalable object storage for application support with high durability and availability.
OpenSearch	Delivers scalable, distributed search and analytics capabilities, powering the application's book search and autocomplete features.

Software

Primary software used to support the Beanstack Digital Platform include the following:

Software	Purpose
Google Workspace	Provides cloud-based productivity and collaboration tools (e.g., Gmail, Docs, Drive) to support communication, document sharing, and team collaboration.
Slack	Enables real-time messaging and collaboration through channels, direct messaging, and integrations, supporting organized communication and operational transparency.
GitHub	Hosts source code repositories with Git-based version control, enabling collaborative development, code review, and continuous integration.
Asana	Facilitates project and task management by enabling teams to plan, track, and manage workflows for improved productivity and accountability.
Insperity	Provides human resources management services, including payroll, benefits administration, and compliance support.
New Relic	Provides application performance monitoring, log aggregation, and infrastructure observability to support system reliability, performance analysis, and incident response.
Sentry	Monitors application errors and exceptions in real time, enabling developers to identify, troubleshoot, and remediate issues that impact system performance and user experience.
HubSpot	Delivers customer relationship management (CRM), sales pipeline tracking, and customer support capabilities to support stakeholder engagement and operational workflows.
Stripe	Provides secure payment processing services for online donations and fundraising contributions, supporting payment authorization, settlement, and transaction management.
Zoom	Provides video conferencing and virtual meeting capabilities to support internal collaboration, customer communications, and remote engagement activities.
Calamari	Offers workforce management functionality for tracking employee time, attendance, leave requests, and vacation planning.

People

Beanstack maintains a staff of approximately 75 employees and contractors across the functional areas of Executive Management, Software Development, IT Security and Compliance, Marketing, Sales, Customer Success and Support, Product Management, Design, and Business Operations.

Executive Management

The Executive Management team incorporates the following individuals:

- Chief Executive Officer (CEO)
- Chief Technical Officer (CTO)
- VP of Product & Client Engagement
- Sr. Director of Marketing
- Sr. Director of Sales
- Sr. Director of Strategy & Operations
- Sr. Director of Design

Executive Management is responsible for developing and implementing strategic initiatives, addressing legal/regulatory requirements, and overseeing their respective teams.

Technology and R&D

The CTO oversees the platform engineering team, software development quality team, and all engineers. The platform engineering team sets the vision and path on future technologies, processes and tools while the software development quality team ensures the application of the standards set by the platform engineering team are applied across all projects. The engineers build and design datasets, applications, backend infrastructure for all the projects and customer deliverables.

Sales

The Sr. Director of Sales oversees direct sales activities. The account executives that make up the sales team conduct outbound emailing, calling, and networking activities to generate new clients for the Company.

Marketing

The Sr. Director of Marketing oversees all marketing activities for the Company, including the marketing website, events, digital outreach and content, social media, and client engagement.

Client Success

The VP of Product & Client Engagement oversees the product management team that manages the product roadmap as well as the client success functions that support school and library clients. The School and Library Success teams are responsible for strategic consultation with clients that empowers them to have success with Beanstack. The Support & Operations team fields all technical and functionality inquiries from clients.

Business Operations

The Sr. Director of Strategy & Operations oversees accounting, board reporting, financial planning & analysis, tax, and accounts payable and receivable operations.

Design

The Sr. Director of Design oversees all product UX/UI design of the Beanstack product and develops and maintains the marketing website. They work closely with the Technology, Product, and Marketing teams.

Data

Beanstack classifies data based on the degree of confidentiality required using the following labels:

- **Confidential:** Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner or Company executive.
- **Internal:** Beanstack proprietary information requiring thorough protection; access is restricted to employees with a “need to know” based on business requirements. This data can only be distributed outside the Company with approval.
- **Public:** Documents intended for public consumption which can be freely distributed outside Beanstack.

Any data file or printed document that is not labeled is classified as “Internal” and handled accordingly.

Beanstack uses AES-256 server-side encryption provided by AWS to store sensitive application configuration and encrypt application data at-rest. To keep data encrypted at-rest, Beanstack ensures that all new resources use AWS server-side encryption.

Policies and Procedures

The following security policies and procedures are maintained and updated at least annually by Beanstack:

- Code of Conduct
- Business Continuity Plan (BCP)
- Data Backup and Disaster Recovery Plan
- Change Management Policy
- Operational Incident Management Plan
- Risk Assessment Policy
- Vendor Management Policy
- Acceptable Use Policy
- Application Performance and Resource Audit Standard
- Application Performance Standards and Objectives
- Artificial Intelligence Acceptable Use Policy
- Incident Response and Remediation Plan
- Written Information Security Plan (WISP)
- Cryptography Policy
- Data Privacy Impact Assessment Report
- HR Security Policy
- Information Classification and Destruction Policy
- Procedure for Secure Ingestion and Purge of Temporary Data
- Software Development Lifecycle (SDLC)

Beanstack employees and contractors are required to acknowledge their understanding of the policies and procedures upon hire.

Complementary User Entity Controls (CUECs)

Beanstack's controls cover only a portion of overall internal control for each user entity of the Beanstack digital platform. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Beanstack. Therefore, each user entity's internal control should be evaluated in conjunction with Beanstack's controls, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal controls to determine whether the identified CUECs have been implemented and are operating effectively.

- User entities must enforce strong authentication policies (e.g., complex passwords and MFA) via their configured SSO providers (Clever, ClassLink, Google, etc.).
- User entities must ensure the secure storage and management of administrative credentials to prevent unauthorized access to Beanstack.
- User entities are responsible for the timely deactivation of accounts for personnel (teachers, staff) who have terminated employment or transitioned to roles no longer requiring access.
- User entities are responsible for assigning appropriate roles and "Least Privilege" permissions to their staff.
- User entities must notify Beanstack of significant changes to their network environment or rostering systems (e.g., shifting from Clever to ClassLink) that could impact data sync integrity.
- User entities are responsible for securing and monitoring the workstations and mobile devices used by their staff and students to access the service.

Complementary Subservice Organization Controls (CSOCs)

Beanstack's primary hosting is with Heroku, a Platform-as-a-Service subsidiary of Salesforce, and Amazon Web Services (AWS), a leading provider of on-demand cloud computing services. The cloud technology provided by these two hosting vendors allows the Company to utilize scalable, highly available computing clusters accessed via the Internet.

Beanstack's services are designed with the assumption that certain controls will be implemented at Heroku and AWS. Such controls are called complementary subservice organization controls. It is not feasible for the service commitments, system requirements, and applicable criteria related to the Beanstack digital platform to be achieved solely by Beanstack. Therefore, each user entity's internal control must be evaluated in conjunction with Beanstack's controls, considering the related CSOCs expected to be implemented at the subservice organizations, as described below:

- Heroku and AWS are responsible for restricting data center access to authorized personnel.
- Heroku and AWS are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
- Heroku and AWS are responsible for the installation of fire suppression, detection, and environmental monitoring systems at the data centers.
- Heroku and AWS are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterrupted power supply.
- Heroku and AWS are responsible for overseeing the regular maintenance of environmental protections at data centers.

Beanstack validates the security posture of its subservice organizations by reviewing the available independent audit reports provided by Heroku and AWS. In addition, through its Vendor Management Policy and operational activities, Beanstack actively monitors the services performed by Heroku and AWS by reviewing the status page alerts and conducting annual compliance checks to ensure controls are functioning effectively. Beanstack also maintains communication with the subservice organizations to stay up-to-date on planned changes at the hosting facilities and communicate any issues or concerns to subservice organization management.

SECTION IV

DESCRIPTION OF THE PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS OF THE BEANSTACK DIGITAL PLATFORM

DESCRIPTION OF THE PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS OF THE BEANSTACK DIGITAL PLATFORM

Principal Service Commitments and System Requirements

Beanstack designs its operational framework to consistently meet its service commitments, ensuring the security of customer data. Commitments to user entities are documented and communicated in service agreements and in the description of the service offerings provided online. This system relies on linking every external promise to a specific, auditable internal policy.

External Commitments (The Promises)

Our documented service agreements and policies include, but are not limited to, the following commitments:

- **Security of User Data:** Using commercially reasonable and appropriate safeguards, including encryption at rest and in transit, and Role-Based Access Controls (RBAC) to limit data access.
- **Incident Notification:** Promptly notifying customers of security incidents or data breaches, as governed by our formal Security Incident Response Plan.

Operational Requirements (The Internal Evidence)

The achievement of these commitments and other system requirements is supported by a comprehensive suite of organizational policies and system requirements communicated throughout our platform.

- **Governance and Oversight:** The Written Information Security Plan (WISP) acts as the organization's security charter, establishing the program, defining scope, and assigning responsibilities (e.g., CTO as Security Officer).
- **System Design and Development:** Our Software Development Lifecycle (SDLC) and Change Management Policy mandate that security and performance controls are integrated into every code change. This includes mandatory peer reviews, automated Brakeman/Dependabot security scanning, and adherence to the Cryptography Policy.
- **Data Management:** The Information Classification and Destruction Policy defines the data lifecycle, ensuring adherence to data minimization principles and timely, secure destruction of Personally Identifiable Information (PII).
- **Vendor Management:** The Vendor Management Policy establishes the requirements for vetting and monitoring all third parties (e.g., AWS, Stripe, and subprocessors) to ensure their compliance supports our overall security commitments.

In addition to these policies, standard operating procedures have been documented to carry out specific manual and automated processes required in the operation and development of the Beanstack digital platform.