Security in Journey.do

At Journey.do, we understand that trust begins with security. Our robust security measures ensure that your data is always safe, protected, and handled with care. From implementing advanced encryption standards and secure authentication methods to providing detailed audit trails, we take every precaution to maintain the integrity of your information.

We also prioritize transparency and accountability, adhering to the highest privacy and security standards like GDPR, SOC-2, and ISO certifications. By leveraging cutting-edge infrastructure through AWS and maintaining strict organizational protocols, we create a secure environment for every interaction. With Journey.do, you can have confidence in a platform designed to safeguard your data while delivering personalized care and exceptional service.

Written Information Security Policy (WISP)

Our Written Information Security Policy (WISP) outlines how we protect your data with clear protocols for access, encryption, and incident response, ensuring compliance with the highest industry standards. It’s a testament to our commitment to safeguarding your information and maintaining your trust.

If you would like to receive a copy of Journey.do’s latest WISP, please send a request to support@lifelabstudios.org. Since an NDA is required, please include your company’s full name, company address, and place of incorporation.

PRODUCT SECURITY

Audit Logs

Every interaction on the platform is logged with detailed tracking of user actions, changes to data, and timestamps, ensuring full traceability and accountability.

Multi-factor Authentication (MFA)

Journey.do provides advanced account protection through MFA using One-Time Passwords (OTP) and Google Authenticator. For environments like detention facilities, innovative Two-Factor Authentication (2FA) options allow officers to generate and share authentication codes securely with youth.

Role-based Access Control (RBAC)

Journey.do is deployed with various defined user roles with respective permissions; however, administrators have control over user roles, permissions, and access. RBAC ensures users can access only data and features relevant to their roles.

Secure Transmission and Sessions

All data transmissions are encrypted via SSL/TLS, ensuring secure connections. Individual sessions are uniquely tokenized and re-verified for security.

DATA SECURITY

Encryption

- **Data at Rest**: Encrypted using AES-256, ensuring sensitive information remains secure.
- **Data in Transit**: Encrypted using HTTPS/TLS 1.2 or newer.

Password Security

Users' account passwords stored only in hashed form, using bcrypt with a modern industry standard work factor.

Generative AI Protections

At Lifelab Studios, we ensure that AI enhances our services without compromising privacy, safety, or fairness. No data is shared externally or used internally to refine or retrain AI models.

1. **No Data Retention**: All data, including user stories, is processed securely and is not stored by our AI systems after use.
2. **Restricted Access**: All data remains within our private cloud instance, with no external sharing to third-party entities.
3. **Generative AI Protections**: Our AI systems leverage external data sources to refine models, generate insights, and provide solutions. However, user data is never used to train or enhance AI technologies outside of the platform.
4. **Bias Prevention & Human Oversight:** No AI-generated insights, assessments, or recommendations are shared directly with users without human review. All AI-generated recommendations are first reviewed by staff, and can be challenged, adjusted, or overridden by staff, ensuring that each decision is personalized and contextually appropriate. Growth and transition plans undergo further review by local officers to ensure they align with best practices and individual needs. Our AI models are designed with fairness in mind, focusing on the specific needs of the populations we serve while actively monitoring and mitigating bias.

Data Retention and Transparency

Journey.do collects and securely stores personal data only for as long as necessary to support users' growth journeys. Users or guardians may request data deletion at any time by contacting support@lifelabstudios.org. Requests are reviewed in compliance with legal and contractual obligations. In cases where data retention is required (e.g., court-mandated programs or compliance reporting), users will be informed of the retention period and how their data is protected.

Data Deletion

Upon **program completion**, user accounts are **archived**, maintaining secure storage within our **SOC 2-compliant AWS infrastructure**.

- **Retention Period**: User data is retained for **up to three (3) years** following program completion to fulfill reporting requirements and support long-term impact evaluations. Upon request, counties may opt for a shorter retention period.
- **Data Eradication**: After the **three-year retention period**, all **personally identifiable information (PII) is redacted**, ensuring that individual users and their actions can no longer be traced.
- **Security Protections**: During the retention period, all archived data remains protected by **industry-standard encryption and access controls**, preventing unauthorized access or misuse.

PRIVACY

Privacy Policy

Journey.do's Privacy Policy outlines how personal data is collected, used, retained, and protected. We adhere to GDPR, CCPA, and other applicable legal requirements, ensuring users have rights including data access, correction, and deletion.

Visit our privacy policy here.

Data Ownership

Users retain ownership of their data, and Journey.do has no rights beyond those necessary for service functionality.

Visit our terms of use policy here.

INCIDENT MANAGEMENT AND RESPONSE

Incident Response Plan (IRP)

Journey.do employs a structured IRP to classify incidents into low, medium, high, or critical levels, ensuring timely communication and resolution.

Data Breach Notification

In the event of a suspected or confirmed data breach, Journey.do will promptly investigate and take immediate action to mitigate any risks. Affected parties will be notified within 24 hours of confirmation of the breach, in accordance with applicable laws and regulatory requirements. Notifications will include the nature of the breach, affected data, steps taken to resolve the issue, and recommended actions for impacted users.

ORGANIZATIONAL SECURITY

Employee Security Training

All employees undergo comprehensive onboarding and annual security training to ensure adherence to confidentiality, privacy, and security policies. A formal employee termination notification process exists, which is initiated by our Human Resources (“HR”) department. Upon notice by HR, all physical and system accesses are promptly revoked.

Principle of Least Privilege

Access to systems is limited to legitimate business needs, reviewed periodically, and revoked immediately upon termination.

Physical Access Control

Robust physical security controls restrict access to offices and data centers, which are managed by AWS with biometric scanning, 24/7 surveillance, and other safeguards.

BUSINESS CONTINUITY

Business Continuity and Disaster Recovery Plans

Journey.do ensures 99.99% uptime with geographically dispersed AWS data centers, offsite backups, and robust failover systems.

Data Backups

Data backups are securely stored in AWS environments, ensuring high availability and disaster recovery.

Quality Assurance Testing (QA)

Journey.do follows a change management process for changes to the production environment. All code changes must undergo a peer code review and include automated unit, functional, and security testing. Testing is performed after deployments to validate application functionality. If validation fails, the application is rolled back to its previous version.

Service Monitoring

Journey.do uses industry-standard systems to monitor its systems to detect service-related issues. The Journey.do team is alerted 24/7 when the threshold criteria are exceeded.

INFRASTRUCTURE SECURITY

Platform Hosting

Journey.do's infrastructure operates on Amazon Web Services (AWS) within the United States.

AWS data centers maintain extensive compliance certifications including ISO 27001, ISO 27017, ISO 27018, ISO 27032, HIPAA, FedRAMP, SOC-1, and SOC-2.

Multi-Tenant Architecture

Journey.do employs a multi-tenant architecture where each customer's data is logically segregated from others. All data is encrypted at rest using AES-256 encryption standards.

ISO 27001 – Data Center

ISO 27001 – Data Center AWS data centers maintain certification with ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, and ISO 27701:2020 standards.

SOC 2 Type II — Data Center

AWS data centers hold SOC 2 Type 2 certification across Security, Confidentiality, Availability, and Privacy Trust Principles.

Physical Access Control – Data Center

For detailed information about AWS's security infrastructure and controls, please refer to AWS's Security Controls Documentation at https://aws.amazon.com/compliance/data-center/controls/

Availability and Reliability

Journey.do utilizes Amazon Web Services (AWS), the world's leading cloud platform, operating across multiple geographically dispersed data centers. Each facility employs comprehensive physical security controls including 24/7 security personnel, video surveillance, multi-factor authentication, and biometric access systems. Redundant power, cooling, and network connectivity ensure high availability, with a service level commitment of 99.99%. All facilities maintain SOC 2 compliance and implement industry-standard fire suppression systems. We have designed our particular service for high availability; no less than 99.85%.

Security Roadmap

Journey.do operates within **Amazon Web Services (AWS), a SOC 2-compliant cloud environment**, ensuring a **secure and reliable infrastructure** for all users while following industry-leading security practices. Designed to support **behavioral change programs in justice, recovery, and related sectors**, our platform upholds best-in-class security measures, including encryption for data at rest and in transit, strict AI safeguards that prevent data storage or model training, role-based access control (RBAC), multi-factor authentication (MFA), and a multi-tenant architecture to maintain data integrity and privacy.

While our current security framework meets the highest standards for the type of data we manage today, our long-term roadmap includes expanding into areas such as **insurance-based payments and managing more sensitive client data related to clinical health and behavioral care**. As we grow, we are **actively working towards full SOC 2 compliance** and further strengthening our **HIPAA-ready capabilities** to support evolving customer needs.

Our **HIPAA-compliant division** supports enterprise customers who need child custody and insurance-based payments, ensuring customers who require HIPAA compliance operate within a **secure technical infrastructure**. For those needing a **HIPAA-compliant architecture**, we offer **single-tenant options** and require a **Business Associate Agreement (BAA)** to ensure proper compliance.

For more information or to request additional documentation, contact us at support@lifelabstudios.org.