Security and Trust Overview

Effective Date	April 20, 2026
Last Modified	April 20, 2026
Policy Status	Active

PsyData Labs L.L.C.

Overview

PsyData Labs L.L.C. is committed to maintaining the highest standards of security, privacy, and ethical responsibility across all services, products, and platforms.

Our approach combines technical safeguards, organizational controls, and governance frameworks to protect data and ensure system integrity.

Security Program

Our security program is built on industry best practices and includes:

- Encryption of data in transit and at rest
- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Continuous monitoring and logging
- Secure development lifecycle (SDLC) practices
- Regular system updates and patching

Data Protection

We implement strong safeguards to protect all categories of data, including:

- Personal data
- Behavioral and analytical data

- Identity verification (KYC) data
- Biometric data
- Health-related data (where applicable)

Data is handled in accordance with our Privacy Policy, Data Processing Agreement (DPA), and Business Associate Agreement (BAA), where applicable.

Infrastructure & Hosting

Our Services are supported by secure infrastructure providers that offer:

- Redundant and resilient systems
- Physical and environmental security controls
- Network security protections
- High availability architecture

Access Control

We enforce strict access management policies:

- Least privilege access
- Role-based permissions
- Access reviews and monitoring
- Immediate revocation upon termination

Incident Response

We maintain a structured Incident Response Plan designed to:

- Detect and respond to security incidents
- Contain and remediate threats
- Notify affected parties where required
- Continuously improve security posture

Vendor Security

All third-party vendors are subject to:

- Risk assessments and due diligence
- Contractual security obligations
- Ongoing monitoring

We maintain oversight of all subprocessors involved in data processing

AI Governance and Ethical Use

Given our focus on artificial intelligence and behavioral systems:

- AI systems are evaluated for bias and risk
- Human oversight is maintained for high-risk use cases
- Sensitive data is protected with enhanced safeguards
- AI outputs are not treated as guaranteed or authoritative

Compliance and Standards

Our practices aligns with:

- Applicable data protection laws
- HIPAA requirements (where applicable)
- Industry-standard security frameworks

Data Retention and Deletion

We retain data only as long as necessary, and securely delete it when no longer required, in accordance with our Data Retention & Destruction Policy

User Responsibilities

Users are responsible for:

- Maintaining the security of their accounts
- Using Services in compliance with our Terms of Service and Acceptable Use Policy
- Reporting suspected security issues

Reporting Security Issues

If you believe you have identified a security vulnerability or incident, please contact our Security team immediately:

Email: security@psydata.org

Documentation and Resources

The following documents support our security and privacy program:

- Terms of Service
- Privacy Policy
- Data Processing Agreement (DPA)
- Business Associate Agreement (BPA)
- Acceptable Use Policy (AUP)
- Cookie Policy
- Subprocessor List

Continuous Improvement

Security is an ongoing process. PsyData Labs L.L.C> continuously evaluates and enhances its practices to address evolving threats and technological changes.

Contact Information

Registered Address:

PsyData Labs L.L.C.
3019 State Route 31
Canastota, NY 13032

Contact Email: contact@psydata.org
Abuse & Report Email: abuse@psydata.org
Legal Email: legal@psydata.org
Privacy Email: privacy@psydata.org
Data Protection Officer Email: privacydpo@psydata.org

Statement of Trust

PsyData Labs L.L.C. is committed to building secure, reliable, and ethical systems at the intersection of technology, artificial intelligence, and psychology.