SOC 2
Controls List

Trust Services Criteria (TSC)
Control Areas

bright defense

ADDRESS

9415 Culver Blvd, #2,
Culver City, CA. 90232

PHONE

(888) 575-3088

PHONE

www.brightdefense.com

01

Security Controls

- Multi-factor authentication
- Web application firewalls
- Detection and monitoring procedures for unauthorized activity
- Physical safeguards for server rooms
- Hiring and background checks for staff in sensitive roles
- Security awareness training for all employees

02

Privacy Controls

- Obtain consent before collecting data
- Limit data collection to what is necessary
- Collect data through lawful methods
- Use data only for the purpose stated
- Dispose of data once it is no longer needed, following internal compliance process requirements
- Maintain documentation as part of internal control responsibilities

03

Confidentiality Controls

- Data classification policies
- Role-based access permissions
- Use of encryption at rest and in transit
- Secure disposal processes for confidential information
- Retention schedules for confidential data

04

Processing Integrity Controls

- Timely error detection and correction during periods of high processing demand
- Input validation and sanity checks
- Monitoring data pipelines to verify inputs and outputs match expected results
- Reconciling processed data through automated checks and reporting
- Controls that prevent unauthorized system components' logic changes
- Automated alerts for processing failures

05

Availability Controls

- Secure backup procedures
- Disaster recovery plans
- Business continuity plans
- Environmental risk management assessments
- Predictive capacity planning as part of a formal readiness assessment

Common Criteria (CC-Series)

- CC1: Control Environment
- CC2: Communication and Information
- CC3: Risk Assessment
- CC4: Monitoring Activities
- CC5: Control Activities
- CC6: Logical and Physical Access Controls
- CC7: System Operations
- CC8: Change Management
- CC9: Risk Mitigation