Prelaunch Group Inc. – Security Whitepaper

Last Updated: August 26, 2025

Overview

Prelaunch Group Inc. is committed to safeguarding the confidentiality, integrity, and availability of our customers' data. This security whitepaper outlines our security practices, controls, and policies designed to protect data and maintain trust with our clients.

Compliance

Our security program is designed around the SOC 2 Trust Services Criteria: Security, Availability, and Confidentiality. We regularly conduct independent audits and penetration tests to validate our security posture.

Infrastructure Security

- Hosted on Amazon Web Services (AWS) in secure, compliant data centers.
- High availability architecture with redundancy and automated failover.
- Firewalls, security groups, and network segmentation safeguard systems.
- Continuous vulnerability scanning and patch management for servers and services.

Application Security

- Secure development lifecycle with mandatory code reviews.
- Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) integrated in CI/CD.
- Dependencies are scanned for vulnerabilities using automated tools.
- AWS Inspector continuously scans workloads and container images for vulnerabilities and security issues.
- Third-party penetration testing conducted annually.
- Rate limiting, WAF, and bot protection applied at the edge.

Data Protection

- Data encrypted in transit using TLS 1.2+ and at rest using AES-256.
- Backups are taken daily, encrypted, and tested regularly for restoration.
- Strict data retention and deletion procedures implemented.
- Customer data is logically segregated to ensure multi-tenancy security.

Access Control & Identity Management

- Multi-factor authentication (MFA) is required for all internal and administrative accounts.
- Role-based access control (RBAC) with least privilege principle enforced.
- Centralized identity management integrated with SSO providers.
- Access logs are maintained and reviewed regularly.
- Automated deprovisioning when employees leave the company.

Monitoring & Incident Response

- 24/7 monitoring of infrastructure, applications, and logs with automated alerting.
- AWS GuardDuty provides continuous threat detection across AWS accounts, analyzing VPC flow logs, DNS logs, and CloudTrail events.
- Security Information and Event Management (SIEM) implemented for real-time analysis.
- Documented incident response plan with defined roles and escalation process.
- Root cause analysis (RCA) performed after each incident with corrective actions tracked.

Vendor & Risk Management

- Critical vendors are reviewed for security practices before onboarding.
- Data Processing Agreements (DPAs) in place where required.
- Annual vendor reviews are conducted to ensure continued compliance.
- Cloud service providers such as AWS are leveraged for their strong security posture.

Employee Training & Awareness

- Mandatory onboarding and annual security training for all employees.
- Regular phishing simulations to raise awareness.
- Engineers receive role-specific training on secure coding and infrastructure hardening.
- Security updates and alerts are communicated via internal channels.

Business Continuity & Disaster Recovery

- Disaster Recovery (DR) plan tested annually with documented outcomes.
- Data backed up daily and replicated across multiple regions.
- Critical services are designed with fault tolerance and redundancy.
- Regular tabletop exercises conducted to prepare teams for crisis situations.

Conclusion

Security is a core value at Prelaunch Group Inc. We continuously enhance our security controls and practices to stay ahead of emerging threats. This document reflects our commitment to protecting customer data and ensuring operational resilience.