Annex II – Security Measures

This Annex forms part of the Data Processing Agreement (DPA) between Rizer Inc. ("Processor") and the Customer ("Controller/Business").

Rizer maintains appropriate **technical and organizational measures (TOMs)** to protect Customer Data against unauthorized or unlawful processing and accidental loss, destruction, or damage, as required under **GDPR Article 32**, **CCPA/CPRA**, and applicable security frameworks (ISO 27001/27701, SOC 2).

---

1. Access Controls

- **Role-Based Access Control (RBAC):** access granted only as needed ("least privilege").
- **Multi-Factor Authentication (MFA):** required for all administrative and production accounts.
- **User Authentication:** unique credentials for each user; password strength enforcement.
- **Session Management:** automatic timeout and revocation on inactivity.

---

2. Data Encryption

- **In Transit:** all data transmitted using TLS 1.2+ / TLS 1.3.
- **At Rest:** Customer Data encrypted with AES-256 or equivalent.
- **Key Management:** secure key rotation and restricted access.

---

3. Logging, Monitoring & Auditing

- **Audit Trails:** access and activity logs maintained for critical systems.
- **Intrusion Detection/Prevention:** monitoring for anomalous activity and brute force attempts.
- **Regular Log Reviews:** centralized SIEM tools used for detection and alerts.

---

4. System and Network Security

- **Segregated Environments:** production, staging, and development environments logically separated.
- **Firewall & WAF Protections:** network firewalls and web application firewalls filter malicious traffic.
- **DDoS Protections:** rate limiting and anti-abuse controls in place.
- **Patch Management:** regular updates to operating systems, frameworks, and libraries.

---

5. Data Management & Retention

- **Data Minimization:** only necessary Customer Data is collected and retained.
- **Backups:** regular encrypted backups with a rolling retention period (≤35 days).
- **Data Deletion:** Customer Data deleted within 30 days of account termination, unless legally required to retain.

---

6. Incident Response & Breach Notification

- **Incident Response Plan:** defined roles and documented escalation paths.
- **24/7 Monitoring:** alerts for unauthorized access or system compromise.

- **Breach Notification:** Customer notified without undue delay, and within **72 hours** where required by GDPR.

---

7. Business Continuity & Disaster Recovery

- **High Availability:** redundant infrastructure to minimize downtime.
- **Disaster Recovery Plan:** recovery time objectives (RTO) and recovery point objectives (RPO) tested periodically.
- **Geographically Redundant Hosting:** critical systems hosted in secure, industry-standard cloud data centers.

---

8. Personnel & Training

- **Confidentiality Agreements:** all employees bound by confidentiality obligations.
- **Security Awareness Training:** mandatory onboarding and annual refreshers.
- **Access Revocation:** immediate removal of access upon role change or termination.

---

9. Vendor & Sub-Processor Security

- **Due Diligence:** security reviews before onboarding sub-processors.
- **DPAs/SCCs:** all sub-processors bound by written data protection terms.
- **Ongoing Monitoring:** periodic reviews of sub-processor compliance and certifications.