Data Security Policy – Rumbl Rentals

Rumbl Rentals (Rumbl Limited Partnership)
Last Updated: 12/08/2025

---

1. Introduction

This Data Security Policy ("Policy") describes the administrative, technical, and organizational measures used by **Rumbl Rentals**, operated by **Rumbl Limited Partnership**, located at **P.O. Box 154, 100 Randall Road, Wrentham, MA 02093** ("Rumbl," "we," "us," "our"), to protect the confidentiality, integrity, and availability of personal information and platform data.

This Policy applies to:

- All Users ("you," "your")
- All Hosts and Guests
- All employees, contractors, and service providers who process Rumbl data
- All systems, databases, and infrastructure supporting the Rumbl Platform

This Policy is incorporated into:

- Rumbl Terms of Service
- Privacy Policy
- Host Agreement
- Guest Agreement

Rumbl is committed to safeguarding user data using industry-leading security practices aligned with applicable laws and standards.

---

2. Guiding Frameworks and Compliance

Rumbl's data security program is informed by globally recognized standards, including:

- **GDPR** (EU/EEA)
- **UK GDPR**

- **CCPA / CPRA** (California)
- **PIPEDA** (Canada)
- **NIST Cybersecurity Framework (NIST CSF)**
- **SOC 2 Type II Principles**
- **ISO/IEC 27001:2022 Information Security Controls**

Rumbl employs reasonable and appropriate safeguards consistent with industry best practices.

---

3. Scope of Protection

This Policy applies to the protection of:

- Personally Identifiable Information (PII)
- Payment-related information (processed by third parties)
- User account data
- Host property information
- Booking data
- Communications and messages
- Analytics, cookies, and tracking data
- Platform logs and metadata
- Internal operational systems
- Device identifiers
- Any other data stored, processed, or transmitted by Rumbl

---

4. Data Classification

Rumbl classifies data into three categories to manage risk effectively:

4.1 Public Data

- Marketing materials

- Website FAQs
- Public Listings (non-sensitive)

4.2 Internal Data

- Operational documents
- Anonymous analytics
- Platform configuration

4.3 Confidential / Restricted Data

- User PII
- ID verification information
- Payment tokens
- Access logs
- Security configurations
- Internal communications

Confidential/Restricted data receives the highest level of protection.

---

5. Encryption and Data Protection Controls

Rumbl uses strong encryption protocols to protect sensitive data.

5.1 Data in Transit

All data transmitted between Users and Rumbl systems is encrypted using:

- **TLS 1.2 or higher**
- HTTPS with HSTS
- Secure cipher suites

5.2 Data at Rest

Confidential data stored in Rumbl systems is encrypted using:

- **AES-256 encryption**
- Key management via secured, access-controlled services

Rumbl does **not** store full credit card numbers; payment information is handled by PCI-DSS–compliant third-party providers (e.g., Stripe).

---

6. Access Controls

Rumbl restricts access to data on a strict, role-based basis.

6.1 Least Privilege

Employees and contractors receive the **minimum access required** to perform their duties.

6.2 Multi-Factor Authentication (MFA)

Required for:

- Admin accounts
- Internal tool access
- Third-party system access

6.3 User Authentication

Users must:

- Create secure passwords
- Protect login credentials
- Maintain updated account information

Rumbl monitors for suspicious login activity.

---

7. Secure Development and Platform Security

Rumbl follows a secure development lifecycle (SDLC) to ensure code integrity.

7.1 Development Practices

- Code reviews for all changes
- Static and dynamic vulnerability scanning
- Dependency vulnerability monitoring
- Separation of development, staging, and production environments

7.2 Application Security Controls

- Rate limiting
- CSRF protection
- Input validation
- Output encoding
- Secure session management
- Anti-bot and anti-automation controls
- Protection against common OWASP Top 10 risks

---

8. Infrastructure and Network Security

Rumbl uses hardened, cloud-based infrastructure with built-in security layers.

8.1 Cloud Security

Rumbl relies on providers with:

- SOC 1, SOC 2, or ISO 27001 certifications
- Physical data center security
- Redundant environments
- DDoS mitigation

8.2 Network Controls

Rumbl implements:

- Firewalls
- Access control lists
- Intrusion detection and monitoring
- IP reputation and anti-fraud surveillance
- Zero-trust principles for internal communications

8.3 Logging and Monitoring

Rumbl logs:

- Authentication attempts

- Admin activity
- Transactional operations
- Security events

Logs are:

- Monitored for anomalous behavior
- Stored securely
- Access-controlled

---

9. Third-Party Service Providers and Vendors

Rumbl uses trusted partners for:

- Payment processing
- Identity verification
- Hosting and cloud storage
- Analytics
- Customer support tools

9.1 Vendor Security Requirements

Vendors must:

- Maintain industry-standard security certifications
- Process data according to Rumbl's Privacy Policy
- Use encryption and secure storage
- Follow confidentiality obligations

9.2 Data Sharing with Vendors

Shared information is limited to:

- Purpose-specific data
- Minimum necessary fields
- Contractually allowed use

Rumbl prohibits unauthorized third-party data sales or misuse.

---

10. User Responsibilities for Account Security

Users must:

- Use strong, unique passwords
- Avoid sharing account credentials
- Update software and devices regularly
- Monitor accounts for unauthorized activity
- Report suspicious behavior immediately

Rumbl may restrict accounts exhibiting suspicious or high-risk activity.

---

11. Incident Response and Data Breaches

Rumbl maintains a formal Incident Response Plan.

11.1 Detection

Rumbl uses automated and manual systems to identify potential:

- Breaches
- Intrusions
- Unauthorized access
- Data leaks

11.2 Containment

Upon detection, Rumbl will:

- Mitigate exposure
- Secure affected systems
- Suspend compromised accounts
- Block malicious traffic

11.3 Investigation

Rumbl will:

- Assess the incident
- Determine scope of impact
- Identify affected Users
- Document findings

11.4 Notification Requirements

Rumbl will notify Users and authorities when required by law, including:

- GDPR (72-hour breach notification)
- CPRA/CCPA
- PIPEDA

Notifications will include:

- Description of incident
- Data potentially affected
- Steps Rumbl is taking
- Guidance for Users (if needed)

---

12. Data Retention and Disposal

Rumbl retains data only as long as needed for:

- Legal and regulatory compliance
- Fraud prevention
- Operational purposes
- Platform safety

12.1 Secure Destruction

When data is no longer required, Rumbl uses:

- Secure deletion
- Cryptographic erasure

- Overwriting techniques
- Vendor-verified destruction

---

13. Fraud Prevention and Risk Controls

Rumbl employs advanced fraud detection mechanisms including:

- Device fingerprinting
- Behavioral analysis
- Payment risk scoring
- Automated flagging of suspicious Listings or accounts
- Monitoring of chargeback patterns
- Identity verification for high-risk accounts

Rumbl may suspend or remove accounts to mitigate fraud.

---

14. User Privacy and Confidentiality

Rumbl:

- Limits internal access to personal information
- Prohibits misuse of personal data
- Ensures employee confidentiality
- Requires vendor confidentiality agreements
- Does not sell personal information

All handling of personal information follows Rumbl's **Privacy Policy**.

---

15. Data Subject Rights (GDPR, CPRA, PIPEDA)

Users may exercise rights related to:

- Access

- Correction
- Deletion (“right to be forgotten”)
- Restriction of processing
- Data portability
- Opt-out of certain processing
- Withdrawal of consent

Requests can be sent to:
admin@rumblrentals.com

Rumbl may require identity verification prior to fulfilling requests.

---

16. Employee Training and Security Awareness

Rumbl requires:

- Regular security training
- Privacy and compliance training
- Phishing simulations
- Incident response training
- Secure coding education for developers

Every individual with system access must follow Rumbl’s internal security standards.

---

17. Enforcement and Violations

Violations by internal personnel may result in:

- Access revocation
- Disciplinary action
- Contract termination
- Legal consequences

Violations by Users may result in:

- Account suspension
- Restrictions
- Termination
- Reporting to authorities (when required)

---

18. Policy Updates

Rumbl may update this Policy at any time.

Updated versions become effective upon posting.
Users will be notified of material updates when required by law.

---

19. Contact Information

For questions, concerns, or security notifications:

Rumbl Limited Partnership
P.O. Box 154
100 Randall Road
Wrentham, MA 02093
United States
Email: **admin@rumblrentals.com**