GRUMMING · TRUST & SECURITY

Security & Architecture Brief

How Grumming protects customer, stylist and salon data. Prepared for customers, salon partners and investors who need to verify that the platform handles personal information responsibly.

TLS 1.3 encryption Every page and request	**Row-level isolation** Enforced by the database	**No plain-text secrets** Credentials held in a vault	**Azure · Central India** Regional data residency

1. Per-account data isolation

Each person can see and change only their own records. This is enforced inside the database engine itself using PostgreSQL Row-Level Security, so it applies to every request regardless of which part of the application made it. A bug in page code cannot expose another account's data.

- Customer appointments are restricted to the authenticated account that created them.
- Home addresses, phone numbers and appointment notes are never returned to another account.
- Salon owners can read only bookings, services and staff belonging to their own salon.
- Stylists can read only the appointments assigned to them.
- Administrative access is granted through a separate role table, never a flag on the user record.
- The authenticated identity is taken from the verified server session, never from a URL or form field.

2. Credential and secret management

No password or service key exists in readable form anywhere in the platform, its source code or its public website files.

- Passwords are stored only as irreversible cryptographic hashes; they cannot be read back by anyone.
- Sign-up verification codes are hashed before storage and expire after a short window.
- Database credentials, email service keys and administrative tokens live in an encrypted, write-only vault.
- Secrets are injected into isolated server processes at run time and never bundled into browser code.
- Only non-sensitive public identifiers are exposed to the browser.

3. Infrastructure and encryption

Grumming runs on Microsoft Azure. The application is served from a managed cloud runtime and data is stored in Azure Database for PostgreSQL Flexible Server in the Central India region.

- All browser traffic is served over HTTPS with modern TLS; plain HTTP is not accepted.
- Database sessions require encrypted connections.
- Automated backups with point-in-time recovery are enabled on the managed database.
- Transactional email is delivered through Azure Communication Services with a verified sender domain.
- Regional data residency in India for latency and compliance.

4. Continuous verification

Security posture is re-checked automatically rather than asserted once. Three classes of automated checks run against the platform.

- Database checks confirm that every table holding personal data has access restrictions enabled and correctly scoped.
- Application interface checks look for exposed data and missing authorisation on booking, profile and administrative endpoints.
- Software supply-chain checks compare every third-party library against public vulnerability advisories.
- Findings are triaged by severity; dependency advisories are resolved through scheduled package updates.
- Current scan summaries are available to salon partners and investors on request.

5. Physical safety during appointments

Grumming sends professionals into customers' homes, so trust extends past the software.

- Identity and background verification before a stylist can accept bookings.
- Hygiene standards and an in-person skill assessment as part of onboarding.
- An emergency alert channel available during an in-progress visit.
- Reviews can only be left against a real completed booking, preventing fabricated ratings.
- Reporting and blocking controls for both customers and stylists.

6. Responsibility summary

Who is accountable for each layer of the stack.

Layer	Control	Owner
Transport	TLS 1.3 encryption, HTTPS enforcement	Cloud edge
Application	Session verification, input validation, role checks	Grumming
Data	Row-Level Security, least-privilege grants	Grumming
Credentials	Password hashing, encrypted secret vault	Grumming / platform
Infrastructure	Managed PostgreSQL, backups, patching	Microsoft Azure
People	Stylist vetting, safety escalation	Grumming operations

7. Frequently asked questions

Can another customer see my bookings, address or phone number?

No. Every booking is tied to the account that created it and the database refuses any request for a record belonging to a different account, even from a signed-in user or a guessed link.

Can a competing salon see my client list or revenue?

No. Salon data is isolated the same way customer data is. A salon account can read only its own bookings, services and staff.

How are passwords stored?

As irreversible cryptographic hashes. Nobody, including the Grumming team, can read a password back.

Is payment information stored on the platform?

Bookings are paid at the appointment, so card details are not held. Any future online payment will be processed by a certified payment provider.

Where is the data physically stored?

In Microsoft Azure's Central India region, with automated backups.

How do I report a vulnerability?

Email security@grumming.com. Every genuine report is acknowledged and investigated, and responsible researchers face no action.

Security contact: security@grumming.com · **Grumming Salon Services Pvt. Ltd.**