

Spotless Detail Solutions

Information Security Policy

Last updated October 12, 2026 - Public copy: www.spotlessdetailshop.com/security

This policy describes how Spotless Detail Solutions ("Spotless Detail") protects the information we hold about customers, payments and our own business, including bank data we access through Plaid. It applies to everyone who works for Spotless Detail and to every system we use. It is reviewed at least once a year and whenever our systems change.

1. Responsibility

The Owner is responsible for information security: setting this policy, granting and removing access, reviewing vendors, and responding to incidents. Security contact: spotless.dtail@gmail.com.

2. Data we protect

- Customer data: names, phone numbers, emails, service addresses, vehicles, appointment history, messages and photos.
- Payment data: cards are entered on and stored by Stripe. We never see or store full card numbers; we keep only brand, last four and expiry.
- Bank data: transaction data from our own business bank and card accounts, obtained through Plaid for bookkeeping. We never see or store bank login credentials; Plaid handles them.
- Business data: revenue, expenses, payroll records and tax documents.

3. Access control

- Access follows least privilege. Staff get only what their job needs: technicians see only the jobs assigned to them; office and financial data, including all bank data, is limited to the Owner.
- Every person has their own login. Shared accounts are not used.
- Multi-factor authentication is required on every account that can reach business systems or data, including email, hosting, database, payments, banking and Plaid.
- Access is removed the same day someone leaves or no longer needs it, and all access is reviewed quarterly.
- Our own software checks authorization on the server for every request; customers can only see their own records.

4. Encryption and infrastructure

- All traffic to our website, apps and service providers uses HTTPS/TLS.
- Data is stored with established providers that encrypt it at rest: Supabase (database and file storage), Vercel (hosting), Stripe (payments), Twilio (text messages) and Plaid (bank connectivity).
- Plaid access tokens and other API keys are stored only as encrypted server-side secrets. They are never placed in source code, in browsers or apps, or in messages.
- Database access from our software uses server-only credentials; nothing sensitive is exposed

to the public internet.

5. Development and changes

- Code lives in a private repository. Changes are made on separate branches, tested automatically and reviewed before they reach production.
- Database changes are additive and recorded; nothing is deleted or rewritten without review.
- Software dependencies and the services we rely on are kept current. Security updates follow a defined timeline: critical vulnerabilities are patched within 7 days, high within 30 days, and others in the next routine update.
- Software that reaches end of life (no longer receives security updates) is replaced before or when support ends. Work devices and operating systems are kept on automatic updates.

6. Vendors

We only use providers that maintain recognized security programs (such as SOC 2 or PCI DSS) for the services they perform for us, and we give each one only the data it needs. The list is reviewed when we add or change a provider.

7. Data retention and deletion

- We keep data only as long as we need it to serve customers, meet legal and tax obligations, and run the business.
- Bank data is used only for our own bookkeeping and is never sold or shared for marketing.
- When a bank connection is no longer needed, we disconnect it in Plaid and delete the stored access token.
- Customers can ask us to delete their information by contacting us; we will do so unless we must keep it by law.

8. Devices

- Phones and computers used for work have a screen lock and current operating-system updates.
- A lost or stolen device is reported to the Owner immediately, and its sessions and passwords are revoked.

9. Incident response

1. Anyone who suspects a security problem reports it to the Owner right away.
2. The Owner contains it: revokes affected access, rotates keys and passwords, and disconnects affected integrations.
3. We investigate what happened and what data was involved, and fix the cause.
4. We notify affected customers, partners (including Plaid when bank data is involved) and authorities as required by law and our agreements.
5. We record what happened and update this policy if needed.

10. Review

This policy is reviewed at least annually, and whenever our systems, vendors or staff access change.